VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Analýza informační bezpečnosti v univerzitním prostředí a návrh souboru opatření k jejímu zajištění

Analysis of Information Security in the University Environment and Design of a Set of Measures to its Ensuring

Student: Martin Huf
Vedoucí diplomové práce: doc. Ing. Milena Tvrdíková, CSc.

Ostrava 2013

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání diplomové práce

Student: **Bc. Martin Huf**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 1802T001 Aplikovaná informatika

Téma: Analýza informační bezpečnosti v univerzitním prostředí a návrh souboru opatření k jejímu zajištění
Analysis of Information Security in the University Environment and Design of a Set of Measures to its Ensuring

Zásady pro vypracování:

1. Úvod
2. Bezpečnost informačních technologií, standardy a metodologie zajišťování bezpečnosti
3. Průzkum bezpečnosti IS v univerzitním prostředí a analýza výsledků šetření
4. Vyhodnocení analýzy a návrh opatření ke zvýšení bezpečnosti IS
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

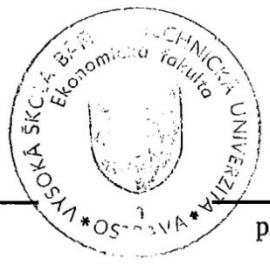
Seznam doporučené odborné literatury:

EGAN, Mark a Tim MATHER. *The Executive Guide to Information Security: Threats, Challenges and Solutions.* Boston: Addison-Wesley Professional, 2004. ISBN 978-03-213-0451-3.
ČERMÁK, Miroslav. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009. ISBN 978-80-7399731-1-1.
DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Milena Tvrdíková, CSc.**

Datum zadání: 23.11.2012
Datum odevzdání: 26.04.2013



Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Místopřísežné prohlášení

Místopřísežně prohlašuji, že jsem celou diplomovou práci vypracoval samostatně. V seznamu použité literatury uvádím veškeré knihy a elektronické zdroje, které byly při tvorbě diplomové práce použity.

Děkuji vedoucímu práce doc. Ing. Mileně Tvrdíkové, CSc. za odbornou pomoc, cenné rady a věnovaný čas při vedení mé diplomové práce.

V Ostravě dne 26. dubna 2013

.....

Bc. Martin Huf

Obsah

1 Úvod

Oblast informační bezpečnosti a jejího zabezpečení se s rozvojem technologií neustále vyvíjí a je potřeba se touto problematikou zabývat a věnovat ji patřičnou pozornost. Například v oblasti mobilních technologií, která je jedním z názorných příkladů. U těchto typů technologií se otázka bezpečnosti za poslední roky stala velmi významnou, především tedy pro běžné uživatele oblíbených moderních mobilních zařízení, tzv. chytré telefony a tablety. Málokoho by ještě před 20 lety napadlo, že taková zařízení, jimiž jsou mobilní telefony, se mohou stát pro uživatele slabým místem bezpečnosti informací. S rozvojem mobilních operačních systémů zároveň dochází k nárůstu bezpečnostních hrozeb, jejichž terčem se stále častěji stávají právě tato zařízení. Uživatelům tak způsobují nepříjemné komplikace či vyvolávají nežádoucí náklady.

Informační technologie jsou nedílnou součástí plnění strategických cílů organizací všeho typu. Proto stále častěji dochází k tomu, že se organizace zabývají problematikou procesního řízení, jehož důležitou část tvoří právě IT. V současné době je na organizace vlivem rostoucí konkurence vyvíjen tlak směrem k větší efektivitě za pomoci standardů, řízení a doporučených postupů. Málokterá organizace dnes, dokáže bez nich efektivně fungovat. Tento trend implementace uznávaných standardů a metod v organizacích neustále roste. I přesto, se málokterá organizace pohybuje v úrovni modelu zralosti řízení procesů výše, než kolem třetí úrovně. Proto by měly organizace vždy část svých peněžních zásob průběžně investovat právě do rozvoje svých ICT, které jsou nejčastějším zdrojem informací. Totéž platí i v problematice informační bezpečnosti, která se může zdát na první pohled jednoduchou a mnohdy opomíjenou problematikou, ale závažnost tohoto tématu je mnohem větší, než si lze představit. Avšak v univerzitním prostředí, které je předmětem této práce, není na jednotlivé univerzity v oblasti informační bezpečnosti a IT obecně vyvíjen takový tlak v souvislosti s uplatňováním standardů a norem. V soukromém sektoru, u kterého je tento tlak vlivem konkurence, jsou často tyto implementace zakončeny následnou certifikací.

Mezi další obávané oblasti z hlediska bezpečnosti patří dnes velice využívané sociální sítě, kde je soustředěno obrovské množství lidí na jednom "místě", a přestavují tak jednoduchý cíl pro potenciální útočníky. Sociální sítě v současnosti ovládají svět Internetu a díky jejich rozmachu s sebou nesou i značné hrozby. Avšak všeobecně platí, že míra bezpečnosti se

odvíjí od chování daného uživatele v prostředí sítě a Internetu. Nesmí se tedy zapomínat na lidský faktor, který je v této oblasti nesmírně důležitým činitelem.

Hlavním cílem diplomové práce je zjistit chování, postoj a povědomí studentů, formou dotazníkového šetření, o zásadách zabezpečení a odpovědností v rámci oblasti informační bezpečnosti obecně i včetně univerzitního prostředí. Dílčím cílem je analýza potenciálních vztahů mezi návyky a chováním uživatelů v síti, pomocí softwarových nástrojů. A na základě výstupů z dotazníkového šetření sestavit návrh možných opatření pro zajištění informační bezpečnosti.

Z hlediska obsahové náplně jednotlivých kapitol se první kapitola zaměřuje na základní teoretické aspekty bezpečnosti informací, včetně stručného popisu uznávaných standardů, praktik a norem. Rovněž jsou zahrnuty základy zabezpečení počítačových sítí. Druhá kapitola je věnována charakteristice univerzitního prostředí, včetně popisu organizační struktury VŠB-TU Ostrava. Dále je popsána úloha útvaru Centra informačních technologií, které tvoří zásadní součást univerzity v oblasti IT. V rámci druhé kapitoly se také nachází analýza informační bezpečnosti v univerzitním prostředí, prostřednictvím dotazníkového šetření včetně jeho interpretace. Třetí kapitola se zaměřuje na vyhodnocení dotazníků a hledání závislostí mezi jednotlivými otázkami a respondenty. Následně jsou popsány současné bezpečností hrozby. Na závěr je sestaven návrh doporučení pro zajištění bezpečnosti informací na univerzitě, s cílem poukázat na možné problémové oblasti, kterým by se měl příslušný útvar univerzity v budoucnu věnovat.

2 Bezpečnost informačních technologií, standardy a metodologie zajišťování bezpečnosti

2.1 Úvod do informační bezpečnosti

V dnešní době již snad neexistuje organizace, která by dokázala fungovat bez ať už jednoduchých, tak sofistikovanějších informačních systémů, které uživatelům, manažerům a vrcholovému vedení poskytují řadu nástrojů pro podporu realizace jejich podnikatelských cílů. Proto je informační bezpečnost ve spojení s informačními systémy nedílnou součástí organizace a její kultury, které se musí každá organizace věnovat ve velkém měřítku. S rozvojem informačních technologií také přímou úměrou rostou bezpečnostní hrozby, které mohou mít pro organizaci velice zásadní vliv na fungování takového podniku. Ať už se jedná o práci prováděnou bez pomoci informačních technologií nebo za její pomoci. Proto má pojem informační bezpečnosti zásadní význam a každá organizace by měla být schopna takové zabezpečení řídit. Alespoň do určité míry, protože v reálném životě neexistuje dokonalé zabezpečení, které by lidi zbavilo všech nástrah, lze se však pokusit tyto bezpečnostní hrozby eliminovat a zajistit kontrolu nad nimi. Do problematiky informační bezpečnosti lze zahrnout vše, co nějakým způsobem souvisí se zabezpečením organizací a jejich obsahu v podobě všech generovaných informací. Zabezpečením informací lze chápat jak softwarové zajištění, tak zajištění hardwarové.

Na informační bezpečnost se dá nahlížet z různých úhlů a obecně tento pojem zahrnuje celou řadu problémů a jejich řešení. Zabezpečení sítě, fyzických spojů a serverů, kódování datových přenosů, digitální podpis, dodržování firemních směrnic, autentizace, autorizace, autenticita, nepopíratelnost, antivirová a antispamová ochrana, hodnocení a ochrana firemních aktiv, analýza rizik, zálohování, obnova po chybě a další.[1]

2.2 Vymezení základních pojmů v kontextu informační bezpečnosti

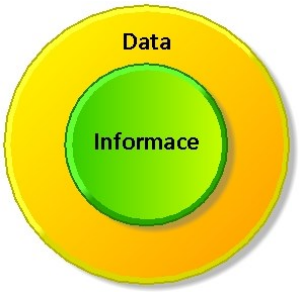
Informace a data

Pojmy data a informace se v praxi často zaměňují nebo slučují. Pro efektivní komunikaci, především mezi odborníky, je třeba tyto různé pojmy odlišit a pokusit se vymezit jejich vztah.

[1] GOGELA, Robert. *Pracovní příručka bezpečnostního manažera.* Vyd. 1. Praha: Česká pobočka AFCEA, 2011, 104 s. ISBN 978-80-7251-364-2.

Data jsou většinou chápána jako statická fakta, časově nezávislá. V praxi se používá také název údaj, přestože pojem údaj je často používán jako obecný výraz pro data i informace. Informace odrážejí stav reality v jiném časovém okamžiku. Smyslem zpracování dat je vytvoření informace. Informace je význam přisouzený datům. Je to, co vyplývá z analýz, zpracování a prezentace dat v takové formě, která bude vhodná pro rozhodovací proces.[2]

Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí stát nutně informací. Pojem data chápeme jako zkratkové profesionální označení pro čísla, text, zvuk, obraz, popř. další smyslové vjemy atd. Tuto skutečnost lze schematicky vyjádřit vztahem množiny a podmnožiny zachycené v následujícím obrázku Obr. 2.1.[3]



Obr. 2.1 Vztah obsahu dat a informací
Zdroj: POŽÁR, Josef. *Manažerská informatika*. 2010

Aktivem je myšleno cokoliv, co má pro organizaci hodnotu. Správné řízení aktiv je pro úspěch organizace životně důležité a je hlavní odpovědností všech úrovní managementu. Aktiva organizace zahrnují fyzická aktiva (např. počítačový hardware, komunikační prostředky, budovy), informace/data (např. dokumenty, databáze), software, schopnost vytvářet určité produkty nebo poskytovat služby, lidé a nehmotné hodnoty (např. abstraktní hodnota firmy, image). Většina nebo všechna z těchto aktiv mohou být považována za dostatečně cenná na to, aby si zasloužila určitý stupeň ochrany. Nejsou-li aktiva chráněna, je nutný odhad rizik, která jsou akceptována. Z pohledu bezpečnosti není možné implementovat a udržovat úspěšný bezpečnostní program, jestliže nejsou identifikována aktiva organizace.[4]

Důvěrnost je vlastnost, že informace není dostupná nebo přístupná neautorizovaným jednotlivcům, entitám, nebo procesům.[5]

---

[2] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, 219 s. ISBN 978-80-7251-250-8.
[3] Tamtéž.
[4] ČSN ISO/IEC TR 13335-1. *Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT*. 1. vyd. Praha: Český normalizační institut, 1999. 24 s.
[5] Tamtéž.

Dostupnost představuje vlastnost, že je něco na požádání přístupné a použitelné autorizovanou entitou.[6]

Dopad je výsledek nežádoucího incidentu, způsobeného buď náhodně, nebo úmyslně, který má vliv na aktiva. Následky mohou mít podobu zničení určitých aktiv, poškození systému IT, a ztráty důvěrnosti, integrity, dostupnosti, individuální zodpovědnosti, autenticity nebo spolehlivosti.[7]

Vlastníkem aktiva je jednotlivec, jemuž byla vedením přidělena odpovědnost za produkci, vývoj, údržbu, použití a bezpečnost aktiv; neznamená to však, že by byl jejich skutečných vlastníkem a měl k nim vlastnické právo.[8]

Aktiva jsou předmětem mnoha typů hrozeb. **Hrozba** má potenciální schopnost způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejich aktiv. Tato škoda se může vyskytnout jako důsledek přímého nebo nepřímého útoku na informace, s kterými pracuje systém nebo služba IT, např. jejich neautorizované zničení, zpřístupnění, modifikace, deformace a nedostupnost nebo ztráta. Aby způsobila poškození aktiv, využívá hrozba existující zranitelnosti aktiv. Hrozby mohou mít přírodní nebo lidský původ a mohou být náhodné nebo úmyslné. Jak náhodné tak úmyslné škody by měly být identifikovány a měla by být odhadnuta jejich úroveň a pravděpodobnost.[9]

Útokem neboli bezpečnostním incidentem, rozumíme buďto úmyslné využitkování zranitelného místa, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech informačního systému, nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Útočit lze přerušením, odposlechem, změnou či přidáním hodnoty k datům.[10]

Integrita je vlastnost, že data nebyla změněna nebo zničena neautorizovaným způsobem.[11]

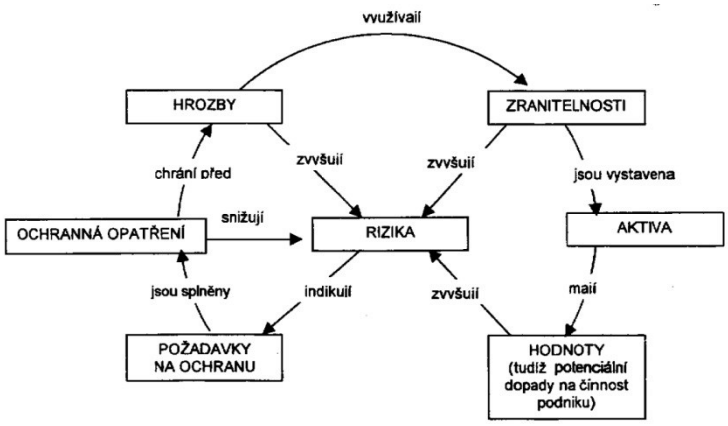
Riziko je potenciální možnost, že daná hrozba využije zranitelnosti, aby způsobila ztrátu nebo poškození aktiv nebo skupiny aktiv, a tedy přímo nebo nepřímo organizace. Jednotlivé nebo vícenásobné hrozby mohou využít jednotlivé nebo vícenásobné zranitelnosti.[12]

---

[6] ČSN ISO/IEC TR 13335-1, ref. 4.
[7] Tamtéž.
[8] GOGELA, Robert, ref. 1.
[9] ČSN ISO/IEC TR 13335-1, ref. 4.
[10] POŽÁR, Josef, ref. 2.
[11] ČSN ISO/IEC TR 13335-1, ref. 4.
[12] Tamtéž.

Zbytkové riziko - rizika jsou obvykle použitím ochranných opatření pouze částečně zmírněna. Částečné zmírnění je vše, čeho je obvykle možno dosáhnout. Z toho vyplývá, že obvykle existují zbytková rizika. Součástí posouzení, zda bezpečnost odpovídá potřebám organizace, je akceptace zbytkových rizik.[13]

Zranitelnosti spojené s aktivy zahrnují slabá místa na úrovni fyzické, organizační, procedurální, personální, řídící, administrativní, hardwaru, softwaru nebo informací. Mohou být využity hrozbami, které mohou způsobit poškození systému IT nebo obchodních cílů. Zranitelnost sama o sobě není příčinou škody; zranitelnost je pouze podmínkou nebo množinou podmínek, které mohou umožnit hrozbě, aby ovlivnila aktiva. Zranitelnosti mohou přetrvávat do doby, než se aktiva samotná změní tak, že se jich zranitelnost dále netýká.[14] Jednotlivé vztahy mezi základními pojmy popisuje obrázek Obr. 2.2.



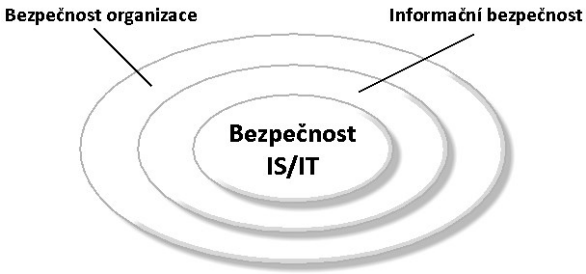
Obr. 2.2 Matice analýzy rizik
Zdroj: ČESKÝ NORMALIZAČNÍ INSTITUT. *ČSN ISO/IEC TR 13335-1*. 1999.

Informační bezpečnost jako obor zabývající se zabezpečením informací v informačních a komunikačních technologiích lze chápat jako systém ochrany dat a informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, fyzických, technických, programových a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot. Můžeme ji definovat jako vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti informačních a komunikačních technologií pro zajištění dostupnosti, důvěryhodnosti a integrity informací.[15]

[13] ČSN ISO/IEC TR 13335-1, ref. 4.
[14] Tamtéž.
[15] POŽÁR, Josef, ref. 2.

V této souvislosti je potřeba ještě zmínit pojmy bezpečnost organizace a informační bezpečnost a rozdíl mezi nimi, což nejlépe vystihuje obrázek Obr. 2.3, který znázorňuje vztah jednotlivých úrovní bezpečnosti v organizaci. Jednotlivé úrovně jsou v podstatě mezi sebou propojené a vzájemně se doplňují. Na nejvyšší obecné úrovni se nachází bezpečnost organizace, která je zaměřena především na bezpečnost majetku a objektů organizace. Další úrovní je informační bezpečnost, jejímž úkolem je zajištění bezpečnosti informací jak digitálního charakteru, tak informací v psané podobě a s tím i spojené procesy v rámci archivace, včetně dodržování termínů vyřazování dokumentů apod. V samotném středu se nachází už konkrétní bezpečnost informačních systémů a informačních technologií, která má za úkol zajistit bezpečnost těch informací, které jsou generovány za pomocí informačních a komunikačních technologií v rámci dané organizace.

Proto je bezpečnost IS a ICT relativně nejužší oblastí řízení bezpečnosti. Ale i přesto je komplikovanou více než dost, protože pracuje s tzv. nehmatatelnými daty, informacemi a službami. Přesto v oblasti informační společnosti je ještě stále mnoho uživatelů, kteří pokládají nehmotná aktiva organizace za bezvýznamná. Cena přenosných paměťových médií je velmi nízká, ale hodnota vlastních dat na tomto médiu může dosahovat vysokých částek i v řádech milionů korun. Hodnotu totiž nemá samotné médium, ale data na něm obsažena.[16]



Obr. 2.3 Vztah úrovní bezpečnosti v organizaci
Zdroj: POŽÁR, Josef. *Manažerská informatika*. 2010

2.3 Frameworky pro řízení informační bezpečnosti

Aplikace metodik, standardů a norem přispává organizacím nejen v budování jejich image v podobě případné certifikace, ale hlavně by to mělo mít příznivý dopad na fungování firmy, zvýšení její efektivnosti a větší konkurenceschopnost na trhu. Tyto metodiky a standardy se často označují jako osvědčené praktiky, tzv. best practice. Uplatňování standardů, norem

[16] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Aleš Čeněk, 2010, 357 s. ISBN 978-80-7380-276-9.

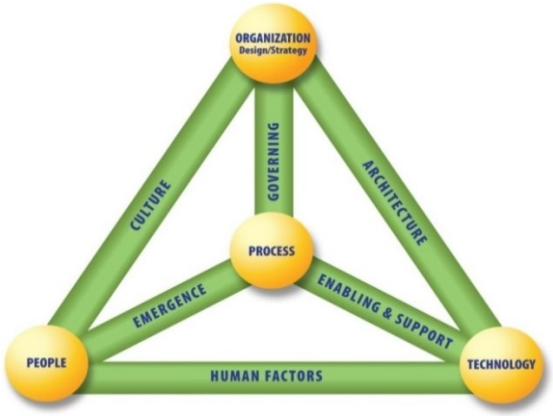
apod. je v dnešní době takřka běžnou praxí. Tyto standardy se hodí především tam, kde vycítíme nedostatky a úzká místa současného stavu. Konkrétní problémy se mohou týkat právě informační bezpečnosti, výkonnosti, efektivnosti a produktivity prováděných procesů nebo spokojenosti zákazníka a jemu poskytovaných IT služeb. Organizace musí být schopna pružně a rychle reagovat na změny v prostředí, ve kterém působí. Zároveň provádět tyto změny s co nejnižšími náklady, což se v dnešní době stává trendem veškerých prováděných změn. V těchto případech je více než vhodné začít přemýšlet nad zavedením některého z uznávaných standardů a metodik, a ten tlak na jejich zavedení se nestále zvyšuje. Stejně tak při pohledu na organizace a jejich procesy v oblasti informačních technologií, které lze řídit pomocí některé z metodik, jako jsou např. ITIL, COBIT, apod. Tyto nástroje jsou běžně označovány jako frameworky a vzájemně tvoří součásti tzv. IT Governance neboli nástroje pro správu a řízení IT. Uplatnění těchto metodik může mít pro organizaci strategický význam. Konktrétně COBIT a ITIL a rozdíly mezi nimi budou podrobněji popsány v dalších částech této práce.

Úkolem IT manažerů je následování celopodnikové strategie a vytváření funkční strategie informačních a komunikačních technologií. Zájem managementu o informační technologie je spojený nejen s ohrožením prosperity a konkurenceschopnosti, ale v krajním případě také vlastní existence podniku. Cíle IT musí být provázány s podnikovými cíli a cíle procesního řízení s cíli IT.[17]

2.3.1 Business Model pro bezpečnost informací

V rámci bezpečnosti informací v organizaci zde také patří zmínka o business modelu pro bezpečnost informací (BMIS - viz obrázek Obr. 2.4), který v roce 2009 vytvořila celosvětová asociace ISACA zaměřující se na problematiku auditu, kontroly a bezpečnosti informačních systémů. Tento model patří do oblasti ISG (Information Security Governance), což se dá přeložit jako správa a řízení bezpečnosti informací, která je v kompetenci vrcholového managementu organizace.

[17] HANÁČEK, Jindřich. Vliv procesního řízení IT na snižování nákladů logistických firem. *IT Systems* [online]. 2010 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/it-pro-logistiku/vliv-procesniho-rizeni-it-na-snizovani-nakladu-logistickych-firem-1.htm



Obr. 2.4 Business Model for Information Security
Zdroj: ISACA. Business Model for Information Security [online], www.isaca.org

Model má podobu úplného grafu a skládá se ze čtyř základních elementů v podobě uzlů, tyto jsou vzájemně spojeny vazbami či hranami, které mají dynamický charakter, a říká se jim dynamické propojení. Původní model BMIS obsahoval pouze tři prvky, kterými jsou lidé, procesy a technologie. Později však byl doplněn o další důležitý prvek organizace s její strategií.

Business model pro bezpečnost informací je tedy tvořen následujícími prvky:[18]

- **Organizace** - řada tradičních modelů obsahuje pouze prvky procesy, lidé, technologie. Prvek organizace se snaží zdůraznit důležitost uspořádání. Prvek organizace je tak chápán jako síť lidí, která využívá procesy pro vzájemnou spolupráci.
- **Procesy** - prvek procesy zajišťuje základní článek propojující všechny formy výměny informací. Procesy jsou vytvářeny tak, aby pomáhaly organizacím naplnit jejich strategické cíle.
- **Lidé** - prvek lidé představuje lidské zdroje, které nějakým způsobem přispívají k činnostem organizace, jako např. zaměstnanci, dodavatelé, výrobci apod. Prvek lidé hraje rozhodující roli v otázce přijatelnosti bezpečnostních opatření.
- **Technologie** - prvek technologie je nejběžnější součástí všech programů pro rozvoj bezpečnosti. Technologie přináší pro řešení bezpečnosti nástroje, které dovolují strategické cíle promítnout do života a usnadnit jejich realizaci.

[18] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

Výše uvedené prvky BMIS modelu jsou dohromady propojeny pomocí dynamických propojení a vytváří tak všestrannou sílu. Akce a chování, které se vyskytují v dynamickém propojení, mohou vyvést model rovnováhy, anebo naopak vrátit jej zpět do rovnováhy. Mezi těchto šest dynamických propojení patří:[19]

- **Správa** - je řízení podniku a vyžaduje strategické vedení. Správa nastavuje hranice, ve kterých podnik působí a je implementován v rámci procesů pro sledování výkonu, popis činností a dosažení shody. Správa zahrnuje zajištění, že podmínky jsou stanoveny a definovány, zjištění, že rizika jsou řízena odpovídajícím způsobem, a ověření, že podnikové zdroje jsou využívány zodpovědně.
- **Kultura** - je vzor chování, přesvědčení, předpokladů, postojů a způsobů, jak věci dělat. Podobné zkušenosti způsobují reakce, které se stávají souborem očekávaných a sdílených chování. Je důležité pochopit kulturu podniku, protože zásadně ovlivňuje, jaká informace je požadována, jak je interpretována a co je třeba s ní udělat.
- **Architektura** - je formální a komplexní zapouzdření lidí, procesů, politik a technologií, které zahrnují podnikové bezpečnostní postupy. Robustní informační architektura podniku je důležitá pro pochopení potřeb zabezpečení a návrhu bezpečnostní architektury. Jde o vzájemné sladění, tak aby technologie byly navrhovány v souladu s podnikatelskými cíli organizace a zároveň byla zajištěna její srozumitelnost.
- **Umožnění a podpora** - dynamické propojení spojuje prvek technologie s prvkem procesy. Jedním ze způsobů, jak pomoci zajistit, aby lidé jednali v souladu s technickými bezpečnostními opatřeními, politik a postupů, je vytvořit použitelné a jednoduché procesy. Transparentnost může pomoci generovat přijetí provádění bezpečnostních kontrol tím, že uživatelům zajistí, aby bezpečnost nebránila v jejich schopnosti efektivně pracovat. Mnoho akcí, které ovlivňují jak technologie, tak procesy, se vyskytují právě v tomto dynamickém propojení.
- **Rozvoj** - je důsledkem růstu a vývoje. Odkazuje na případy, které vznikají v životě organizace a nemají zjevnou příčinu, jejíž výsledky není možné řídit a předvídat. Vznik dynamického propojení mezi prvky lidé a procesy je místo pro zavedení možných řešení, jako jsou zpětnovazební smyčky, srovnání kroku s technologickým

[19] ISACA. *An Introduction to the Business Model for Information Security* [online]. 2009 [cit. 2013-04-17]. Dostupné z: http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf

vývojem, zvážení vznikajících problémů v životním cyklu návrhu systému, řízení změn a řízení rizik.

- **Lidské faktory** - představují interakci a mezeru mezi technologiemi a lidmi, a jsou pro informační bezpečnost i pro udržení rovnováhy v rámci modelu kritickým místem. Pokud lidé nechápou, jak používat technologie, nepřijmou technologie nebo se nebudou držet příslušných bezpečnostních politik, může dojít k rozvoji závažných bezpečnostních problémů, proto je důležité všechny lidi trénovat v příslušných dovednostech. V rámci tohoto propojení se mohou vyskytnout interní hrozby, mezi něž patří např. únik dat, krádež dat či zneužití údajů apod.

Model BMIS je moderní pojetí, které je určeno pro pochopení komplexního pohledu na problematiku bezpečnosti informací. Z těchto důvodů je tento model vhodný i pro použití v rámci modelování.[20]

2.3.2 COBIT

COBIT (Control Objectives for Information and Related Technology) je mezinárodně uznávanou metodikou – rámcem zaměřený na podporu IT Governance, který vytvořila americká mezinárodní organizace ISACA (organizace ISACA již byla zmíněna v části zabývající se Business modelem pro bezpečnosti informací). Opírá se o soubor všeobecně uznávaných praktik řízení informačních a komunikačních technologií tak, aby využití informací a nasazení ICT přispívalo k dlouhodobému rozvoji organizace, prohlubovalo její strategické cíle a snižovalo rizika související s použitím ICT.[21]

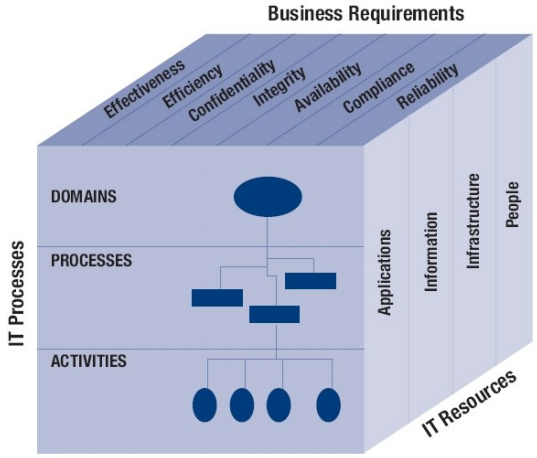
Úplně první verze metodiky COBIT byla vytvořena organizací ISACA v roce 1996. Vydání první a druhé verze metodiky COBIT předcházel analytický výzkumný projekt, jehož účelem bylo sjednocení praktických poznatků a vhodných mezinárodních technických norem a doporučení nejlepší vžité praxe.[22]

Doposud poslední a zároveň současná platná verze COBIT je označována COBIT 5, která byla vydána na začátku roku 2012. COBIT 5 buduje a rozšiřuje metodiku COBIT 4.1 o integraci dalších významných rámců, norem a zdrojů, včetně oblasti pro řízení investic IT

[20] DOUCEK, Petr, ref. 18.
[21] Metodika COBIT: systematický přístup k řízení ICT. *IT Systems* [online]. 2005 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/clanky/metodika-cobit-systematicky-pristup-k-rizeni-ict.htm
[22] DOUCEK, Petr, ref. 18.

(Val IT) a oblasti pro řízení rizik (Risk IT) vyvinuté organizací ISACA, ITIL a souvisejících standardů od mezinárodní organizace pro normalizaci (ISO). Mezi hlavní výhody pro organizace všech velikostí patří zejména optimalizace nákladů na IT služby a technologie, udržování IT rizika na přijatelné úrovni, udržování vysoce kvalitních informací pro podporu obchodních rozhodnutí, dosahování strategických cílů, účinné a efektivní uplatňování technologií atd.

Základní princip metodiky COBIT je postaven na cílech organizací (strategických požadavcích – tzv. Business Requirements), zdrojích informačních technologií (aplikace, informace, infrastruktura, lidé) a procesech IT (na úrovni domény, procesů a aktivit). Tyto tři komponenty využívá tzv. COBIT kostka, která je uvedena na obrázku Obr. 2.5. Současně nejlépe ukazuje základní koncepci metodiky: zdroje informatiky jsou řízeny procesy tak, aby bylo dosaženo stanovených cílů informatiky, které odpovídají strategickým požadavkům. [23]



Obr. 2.5 COBIT kostka
Zdroj: COBIT [online], www.internalaudit.iastate.edu

Při pohledu na kostku COBIT si lze všimnout rozdělení IT procesů na různé úrovně podrobnosti, které se nazývají domény. Nejnovější verze COBIT 5 se skládá z procesů, které jsou rozděleny do dvou oblastí, a celkově obsahují pět domén (oproti COBIT 4.1, který měl čtyři domény) a 37 procesů, které jsou rovněž zachyceny ve schématu uvedeném v Příloze 1:

- Správa IT
  - Hodnocení, směrování, monitorování (Evaluate, Direct and Monitor - EDM)
- Řízení IT
  - Srovnání, plánování a uspořádání (Align, Plan and Organise - APO)

[23] DOUCEK, Petr, ref. 18.

- Sestavení, shromažďování a implementace (Build, Acquire and Implement - BAI)
- Doručení, servis a podpora (Deliver, Service and Support - DSS)
- Monitorování, hodnocení, posuzování (Monitor, Evaluate and Assess - MEA)

COBIT 5 v kontextu informační bezpečnosti poskytuje návod, který pomáhá IT a bezpečnostním profesionálům pochopit, využít, realizovat a řídit důležité informace s bezpečností souvisejících činností, a vytvářet informovanější rozhodnutí se zachováním povědomí o nových technologiích a doprovodných hrozeb:[24]

- Snížit komplexnost a zvýšit efektivnost nákladů
- Zvýšit spokojenost uživatelů s uspořádáním a výsledky informační bezpečnosti
- Zlepšení integrace informační bezpečnosti
- Informovat rizikové rozhodnutí a povědomí o možných rizicích
- Zvýšení podpory pro inovace a konkurenceschopnost

2.3.3 ITIL

První zmínky o ITIL neboli Information Technology Infrastructure Library zasahují do 80. let minulého století, kdy vláda ve Velké Británie oslovila agenturu CCTA za účelem zlepšit řízení informačních technologií ve veřejné správě.[25] Tato agentura měla za úkol ucelit a sjednotit jednotlivé přístupy a vytvořit jakousi praktickou kuchařku globální úrovně pro lepší pochopení i následné znovupoužití těchto přístupů pro organizace různého charakteru. Přičemž první verze ITIL byla sjednocením nejlepších postupů, tzv. best practice, které pramenily z praktických zkušeností nejlepších odborníků v oblast ICT. Agentura CCTA se poté stala předmětem fúze spolu s dalšími britskými agenturami a výsledkem byla nová organizace OGC (Office of Government Commerce), která je pověřena vydáváním nových aktualizací ITIL. Dnes existuje ITIL ve třech verzích, přičemž tou nejnovější je ITIL v3, která byla vydána v roce 2007 a byla vylepšení ITIL v2. ITIL v3 je platný dodnes.

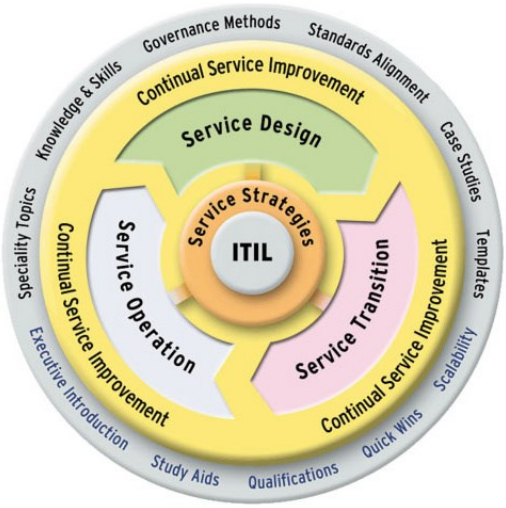
ITIL je procesně orientovaný rámec pro řízení služeb informačních a komunikačních technologií, čímž se také liší od ITIL v2, který byl zaměřen výhradně na procesy. Výhodou tohoto rozsáhlého procesně orientovaného rámce je, že je postaven na nejlepších zkušenostech odborníků z různých firem z celého světa, a proto je také dobře srozumitelný

[24] ISACA. *COBIT 5 for Information Security* [online]. 2012 [cit. 2013-04-17]. ISBN 978-1-60420-255-7. Dostupné z: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf
[25] DOUCEK, Petr, ref. 18.

lidem z praxe, je nezávislý na platformě a používá jednoznačnou terminologii. Jako takový může být dobrou oporou pro manažery ICT služeb, kteří chtějí optimalizovat řízení svého úseku. Pracovníci IT oddělení v těchto knihách najdou doporučené způsoby a procesy, jak nejlépe řídit a spravovat provoz IT, a jak zajistit kvalitní poskytování IT služeb. Pro podporu řízení IT služeb podle rámce ITIL dnes již existuje celá řada softwarových nástrojů. ITIL v podstatě není metodika, ale pouze rámec, proto je nutné tento rámec nejprve implementovat.[26]

V rámci jednotlivých aktualizací také docházelo k redukci obsahu. Poslední verze je seskupena do pěti svazků a vychází z modelu znázorněného na obrázku Obr. 2.6. Model ilustruje životní cyklus IT služeb složený ze strategie služeb až po neustálé zlepšování služeb. Konkrétně těchto pět dokumentů tvoří:

- Strategie služeb
- Návrh služeb
- Implementace služeb
- Provoz služeb
- Průběžné zlepšování služeb



Obr. 2.6 Model ITIL v3 dle OGC

Zdroj: ITIL. ITIL® Knowledge - Overview [online], www.itil.org

Při pohledu na obsahovou náplň ITIL z hlediska bezpečnosti informací, koncepce zařazení problematiky bezpečnosti do zvláštní publikace ve verzi v2 byla často předmětem kritiky. Oponenti poukazovali na to, že bezpečnost informací by měla být součástí každého procesu

[26] HOLEK, Tomáš. Procesní řízení IT služeb. *IT Systems* [online]. 2007 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/sprava-it/procesni-rizeni-it-sluzeb.htm

popisovaného např. v knihách Dodávka a podpora služeb a neměla by být řešena odděleně od vlastního průběhu procesů. Ve verzi ITIL v3 je proces Information Security Management (ISM) součástí Návrhu služeb. Jde o nový proces, který má zajistit důvěrnost, integritu a dostupnost aktiv, informací, dat a služeb IT organizace. Důvěrnost, integrita a dostupnost informací tvoří tři hlavní principy bezpečnosti informací, jak také znázorňuje obrázek Obr. 2.7. Cílem procesu Návrhu služeb je propojení bezpečnosti informací s celkovou bezpečností organizace tak, aby se chránily zájmy všech, kteří jsou závislí na informacích a informačních systémech. Zároveň ITIL v3 intenzivně pracuje s řízením rizik včetně bezpečnostních rizik. Právě přes řízení rizik se bezpečnost promítá do celého životního cyklu IT služeb, znázorněného výše.

Obr. 2.7 Hlavní přístupy bezpečnosti informací
Zdroj: CIA: Důvěrnost – integrita – dostupnost [online], www.cleverandsmart.cz

COBIT i ITIL představují rámce a soubor nejlepších praktik, ale problematice informační bezpečnosti se nevěnují v takové míře, jako je tomu u ISMS (Information Service Management System), kterému bude věnována samotná část práce, protože patří mezi nejzásadnější praktiky v oblasti informační bezpečnosti. V případě využití, COBIT poskytuje praktický manuál především pro vrcholový management ke sledování funkčnosti a efektivnosti IT organizace a pro auditory, kteří mají na starost provádění auditu systému řízení IT. V tomto případě je i nutné připomenout, že COBIT na rozdíl od ITIL pohlíží na oblasti IT v širším a komplexnějším měřítku. Naopak pomocí ITIL jsme schopni řešit různé problémy na detailnější úrovni, i z tohoto důvodu jej využijí především odborníci a manažeři IT.

2.4 Normy pro řízení bezpečnosti informací

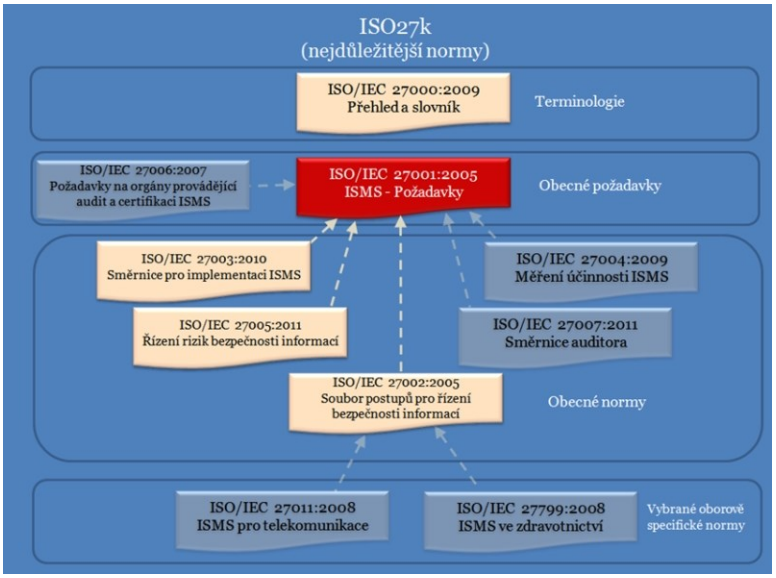
Existuje řada norem, které se buď přímo zabývají informační bezpečností, nebo existují takové, které se této problematiky týkají pouze okrajově. V následujících částech budou, z důvodu rozsahu práce, popsány pouze klíčové normy, zabývající se bezpečností informací. Mezi ty hlavní normy a standardy patří ISO/IEC 27001, ISO/IEC 27002 a ISO/IEC TR 13335. Alespoň pro představu, že norem je opravdu velké množství, lze zmínit další uznávané standardy, jimiž jsou např. ISO/IEC 17799, BS 7799, normy německé organizace GISA, ISO/IEC 18028, ISO/IEC 18044, americký Common Criteria (ISO/IEC 15408), standardy americké organizace NIST, ISO/IEC 19000, ISO/IEC 24000, ISO/IEC 29000, atd.

2.4.1 Řada norem ISO/IEC 27000

Normy mezinárodní organizace pro certifikaci (ISO) postupně vydává nové normy řady 27000 (někdy také označováno jako 27k) či provádí jen jejich aktualizace a revize, které jsou zaměřeny právě na problematiku bezpečnosti informací. Obecným cílem zavádění ISO norem a standardů je zvýšení účinnosti a efektivnosti v daném oboru. V České republice se normalizací zabývá Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ). V některých již existujících normách a standardech jsou implementovány části zabývající se bezpečností informací, takže hlavním cílem bylo jejich vymezení a sjednocení těchto návodů a doporučení do samostatné oblasti norem.

Normy zabývající se bezpečností se staly významným prvkem v oblasti informační bezpečnosti. Každá norma nahlíží na problematiku informační bezpečnosti z různých pohledů, a také se liší v jejich implementaci. Normy zavádí do oblasti informační bezpečnosti důležitý pojem, kterým je systém řízení bezpečnosti informací neboli ISMS (Information Security Management Systém). Většina norem je velice úzce spojena a aplikována právě se systémem řízení bezpečnosti informací (ISMS), kterému bude věnována samostatná část práce. Za klíčové a nejdůležitější normy z řady ISO 27000 lze považovat normy s označením ISO/IEC 27001 (vychází z původní britské normy BS 7799-2) a ISO/IEC 27002 (změna označení z původního ISO/IEC 17799:2005). Obě tyto normy můžeme považovat za základní východiska a specifikaci ISMS. Detailněji budou vysvětleny v části věnující se ISMS. Základní výčet norem řady 27k a jejich základní charakteristiky lze shrnout do přehledu, uvedeného v Příloze 2.

Řada norem pro řízení bezpečnosti informací ISO/IEC 27000 ideově vychází z konceptu PDCA (zkratka je z anglických slov Plan-Do-Check-Act), jejím základem jsou normy, jež jsou uvedeny na obrázku Obr. 2.8. Podobně jako u jiných systémů řízení (např. ISO 9001, ISO 14001) je za jádro normalizace považována definice systému.[27]



Obr. 2.8 Výčet nejdůležitějších norem řady ISO/IEC 27000
Zdroj: Normy ISO27k [online], sites.google.com/site/isoanist/home

Řada standardů je v dnešní době různě propojena a stávají se tak komplexnějšími, jako např. metodika CRAMM, ve které je částečně obsažena norma ISO/IEC 27001.

2.4.2 ISO/IEC TR 13335

Dalším standardem a doporučením, kterým je potřeba se v souvislosti s informační bezpečností zabývat, je norma ISO/IEC 13335. Její obsah je rovněž dostupný i v českém jazyce. Původní podoba normy, neboli správně řečeno rodiny norem ISO/IEC TR 13335, se skládala ze čtyř částí tzv. technických zpráv (od toho zkratka TR – technical reports), které ale prošly revizí a výsledkem je pouze jedna část této normy. Části tři a čtyři byli upraveny a seskupeny do nové podoby normy s označením ISO/IEC 27005:2011.

Část 1 Koncepty a modely bezpečnosti IT poskytuje přehled základních pojetí a modelů, použitých k popisu řízení bezpečnosti IT. Tento materiál je vhodný pro manažery odpovědné za bezpečnost IT a pro ty, kdo jsou odpovědní za celkový bezpečnostní program organizace.

[27] DOUCEK, Petr, ref. 18.

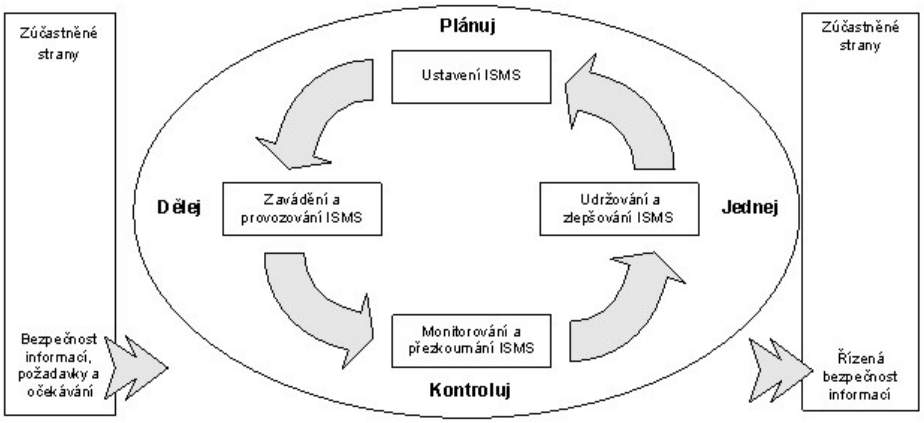
Část 2 Řízení a plánování bezpečnosti IT popisuje řídící a plánovací aspekty. Tato část má význam pro manažery s odpovědnostmi souvisejícími se systémy IT organizace. Těmi mohou být manažeři IT, kteří jsou odpovědní za dohled nad návrhem, implementací, testováním, pořízením nebo provozováním systémů IT nebo manažeři, kteří jsou odpovědní za činnosti, které využívají podstatným způsobem systémy IT. Část 3 Techniky pro řízení bezpečnosti IT popisuje bezpečnostní techniky vhodné pro použití pracovníky, kteří jsou zapojeni do manažerských činností v průběhu životního cyklu projektu, jako je plánování, návrh, implementace, testování, získání nebo provozování. Část 4 Výběr bezpečnostních opatření poskytuje směrnice pro výběr ochranných opatření s ohledem na potřeby činnosti organizace a problémy bezpečnosti a jak může být tento výběr podporován použitím základních modelů a kontrol. Popisuje proces výběru ochranných opatření podle bezpečnostních rizik, problémů a specifického prostředí organizace. Ukazuje, jak dosáhnout odpovídající ochrany a jak může být tento proces podporován aplikací základní úrovně bezpečnosti. Poskytuje i vysvětlení, jak přístup naznačený v této části podporuje techniky pro řízení bezpečnosti IT předložené v ISO/IEC TR 13335-3.[28]

2.5 Systém řízení bezpečnosti informací ISMS

V dnešní době se žádná organizace nemůže obejít bez řízení bezpečnosti informací a postupně se stává důležitou součástí každodenního řízení a vnitřní kultury organizace. Abychom byli schopni řízení bezpečnosti cíleně, účinně a účelně rozvíjet, je potřebné na tento prvek řízení pohlížet jako na systém řízení bezpečnosti informací. Norma ISO/IEC 27001 jej definuje jako část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací. Systém řízení v sobě zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, mechanismy, postupy, procesy a zdroje. Systém řízení bezpečnosti informací je podobně jako ostatní systémy řízení založen na modelu PDCA (Plan-Do-Check-Act). Využití tohoto modelu pro ISMS je zachyceno na obrázku Obr. 2.9, na kterém byly definovány následující čtyři etapy celého životního cyklu systému řízení:[29]

[28] ITIL - Bezpečnost IS/IT. [online]. [cit. 2013-04-17]. Dostupné z: http://itil.cz/index.php?id=1003
[29] DOUCEK, Petr, ref. 18.

- **Ustanovení ISMS** - cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření.
- **Zavádění a provoz ISMS** - cílem této etapy je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace.
- **Monitorování a přezkoumání ISMS** - hlavním cílem této etapy je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací.
- **Údržba a zlepšování ISMS** - cílem poslední etapy je realizace možností zlepšování systému řízení bezpečnosti informací, ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků.



Obr. 2.9 PDCA model aplikovaný na procesy ISMS
Zdroj: ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27001 [online], www.unmz.cz

ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že jsou určena aktiva, která se mají chránit, jsou zvolena a řízena možná rizika bezpečnosti informací, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována. ISMS může být zaveden pro organizační složku instituce, informační systém nebo jeho část, případně může zahrnovat celou organizaci.[30]

[30] GOGELA, Robert, ref. 1.

2.5.1 ISO/IEC 27001

Kompletní název normy ISO/IEC 27001 je **Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky**. Tato norma má podobu množiny požadavků a pro vyjadřování jednotlivých požadavků používá výraz „musí“, který vyjadřuje závaznost daného požadavku. Požadavky normy jsou spojeny s naplněním modelu PDCA, který tato norma zavádí a již byl zmíněn v části věnované ISMS, a všechny jsou závazné, protože společně vytvářejí úplný a smysluplný celek. Zajištění shody s normou ISO/IEC 27001 je podmíněno splněním všech těchto závazných požadavků.[31]

Norma ISO/IEC 27001:2005 definuje požadavky na utajení, integritu a dostupnost informací a ostatních aktiv organice, se kterými organizace přichází do styku, přičemž:[32]

- zajistit utajení (důvěrnost) informací znamená, že k různým druhům informací mají přístup pouze autorizované osoby;
- zajistit integritu informací znamená kontrolovat přesnost a ucelenost informací a metody pro jejich zpracování;
- zajistit dostupnost informací znamená, že autorizovaní uživatelé mají včasný a kompletní přístup ke všem požadovaným datům.

Norma popisuje vhodný systém řízení, strukturu a procesy pro řízení bezpečnosti informací podle opatření definovaných v ISO/IEC 27002. Organizace mohou na základě hodnocení rizik z ISO/IEC 27002 vybrat přesně ta opatření, která jsou aplikovatelná v jejich prostředí. Z tohoto důvodu jsou hlavní části ISO/IEC 27002 uvedeny také v příloze normy ISO/IEC 27001. Podle ISO/IEC 27001 mohou organizace definovat rozsah certifikovaného systému. Správná definice ISMS je kritickým krokem při jeho zavádění v organizaci. Pokud je systém řízení bezpečnosti informací zaveden pouze v určité části organizace, vydaný certifikát je platný právě pro tuto část nikoli pro celou organizaci.[33]

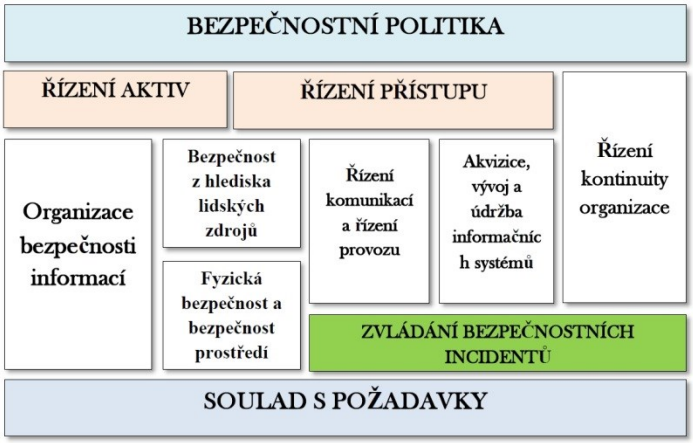
[31] DOUCEK, Petr, ref. 18.
[32] DRASTICH, Martin. *Systém managementu bezpečnosti informací*. 1. vyd. Praha: Grada, 2011, 126 s. Průvodce (Grada). ISBN 978-80-247-4251-9.
[33] RAC. *ISO/IEC 27001:2005* [online]. [cit. 2013-04-17]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27001

2.5.2 ISO/IEC 27002

Norma ISO/IEC 27002 s originálním názvem **Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací** je souborem nejlepších postupů, je navržena jako soubor doporučení a jednotlivé požadavky závazné nejsou. To se odráží i v použití obratu „měl by“. Tato norma představuje druhé základní východisko ISMS, který poskytuje soubor postupů pro řízení bezpečnosti informací (dříve ISO/IEC 17799). Ta obsahuje tzv. nejlepší zkušenosti řízení bezpečnosti informací. Její revidované vydání bylo publikováno v červnu 2005.[34]

ISO/IEC 27002:2005 může být využita jako kontrolní seznam všeho správného, co je nutno pro bezpečnost informací v organizaci udělat. Aktuální verze normy ISO/IEC 27002:2005 je mezinárodně přijatý standard, sbírka nejlepších praktik z oblasti bezpečnosti informací. Norma ISO/IEC 27002 obsahuje celkem 11 základních oddílů bezpečnosti (viz obrázek Obr. 2.10), které jsou dále rozděleny do 39 kategorií bezpečnosti (kontrolních cílů), jež poskytují návod pro ochranu informačních aktiv proti narušení jejich důvěrnosti, dostupnosti a integrity. V podstatě tyto cíle opatření zahrnují funkční požadavky pro architekturu bezpečnosti informací organizace. ISO/IEC 27002 také popisuje nejlepší praktiky pro zajištění bezpečnosti informací, které by organizace měla vzít v úvahu pro zajištění kontrolních cílů. Norma nepřikazuje, která opatření musí být bezpodmínečně aplikována, ale ponechává rozhodnutí na organizaci. Vhodná opatření jsou vybírána na základě hodnocení rizik a jejich implementace je závislá na konkrétní situaci. Cílem není implementovat vše, co norma popisuje, ale spíše naplnit všechny aplikovatelné cíle opatření. Tento přístup zajišťuje, že norma je široce aplikovatelná a dává uživatelům velkou flexibilitu při implementaci. Nicméně toto přináší obtíže při certifikaci, kdy může být složité posoudit, zda jsou aktuální bezpečnostní opatření plně v souladu s normou.[35]

[34] DOUCEK, Petr, ref. 18.
[35] RAC. *ISO/IEC 27002:2005* [online]. [cit. 2013-04-17]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27002



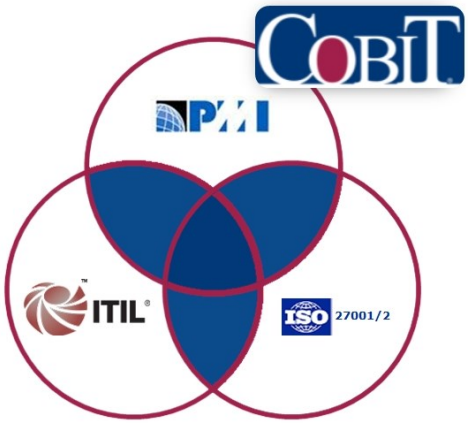
Obr. 2.10 Oblasti informační bezpečnosti dle ISO/IEC 27002

Zdroj: KRAUSOVÁ, Světlana. ISMS dle ISO/IEC 27001 [online], www.krausova.eu

Každé opatření obsažené v této normě se skládá ze tří částí, jimiž jsou Opatření, Doporučení k realizaci a Další informace. Tato opatření jsou zachycena v tzv. myšlenkové mapě bezpečnostních opatření, která vznikla na základě normy ISO/IEC 27001.

2.6 Vztah mezi normami a standardy

Například COBIT se často používá jako nejvyšší úroveň v oblasti správy a řízení IT, poskytující celkový kontrolní rámec založený na procesním IT modelu. Sjednocuje tak soubor postupů a standardů, jimiž mohou být např. norma ISO/IEC 27001 a 27002, rámec ITIL a metodika PMBOK. Jejich prolínání je zachyceno na obrázku Obr. 2.11. Sjednocením standardů a metodik se zlepšuje jejich soulad s podnikatelskými potřebami a integraci mezi nimi, a pokrývá celé spektrum činností souvisejících s IT.



Obr. 2.11 Vztah mezi frameworky a normami

Zdroj: ISACA. COBIT: Transforming Enterprise IT [online], www.isaca.org

2.7 Bezpečnostní politika organizace

Bezpečnostní politika organizace je jedním ze základních pilířů, na kterém stojí úspěšnost systému řízení informační bezpečnosti. Bezpečnostní politika informačních a komunikačních technologií definuje základní bezpečnostní požadavky, nařízení, opatření, postupy, které mají za cíl zajistit ochranu a bezpečnost všech důležitých informací.[36]

Tento vrcholný dokument tvoří špičku pyramidy dokumentů, která pokrývá všechny aspekty bezpečnosti informací od těchto zásad až po technické popisy. Každý koncept uvedený v bezpečnostní politice musí být v podřízených dokumentech konkretizován a/nebo musí být rozpracován.[37]

Bezpečnostní politika musí být definována formou dokumentu a měla by zahrnovat a popisovat vybraná témata z informační bezpečnosti. Tento dokument nejdříve podstupuje proces schválení vedením organizace a měl by být dostupný všem uživatelům ve srozumitelné formě. U prosazování bezpečnostní politiky je velice důležitá podpora právě ze strany managementu. Při zavádění bezpečnostní politiky musí existovat nějaká zpětná vazba, tedy měla by být pravidelně kontrolována a případně aktualizována dle aktuálních potřeb a požadavků či nahodilé změny tak, aby byla zajištěna její účinnost. Každou takovou změnu musí management organizace zaznamenat a následně provést jejich vyhodnocení v daných intervalech. Záleží pouze na organizaci, jak si tyto intervaly pro opětovné zaznamenání a vyhodnocení změn nastaví. Intervaly se mohou lišit v závislosti na závažnosti problematiky, velikosti organizace, strategických cílů apod.

Při vytváření takového dokument bezpečnostní politiky by se měli jeho autoři zaměřit na následující aspekty bezpečnosti informací:[38]

- Definice základních pojmů bezpečnosti informací – jeho cíl, rozsah a význam – prohlášení vedení organizace o záměru podporovat cíle, principy bezpečnosti informací – stručný výklad bezpečnostních zásad, principů, standardů a požadavků – stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací – odkazy na dokumentaci, která politiku bezpečnosti informací podporuje.

[36] DRASTICH, Martin, ref. 32.
[37] SEDLÁČEK, Václav. *Management systému informační bezpečnosti - ISMS: studijní opora disciplíny*. Vyd. 1. Třebíč: Vivat Academia, 2010, 96 s. ISBN 978-80-87385-05-0.
[38] DRASTICH, Martin, ref. 32.

2.8 Bezpečnostní hrozby a rizika v informační bezpečnosti

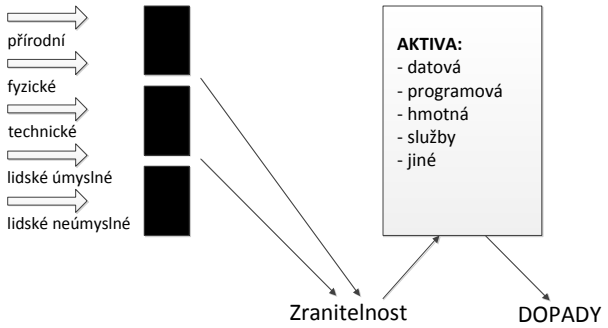
Pojem hrozba již byl definován na začátku této kapitoly. V rámci informačního systému společnosti dochází k vytváření a manipulaci s daty a informacemi všeho typu, které podléhají bezpečnostním hrozbám a incidentům. Při nedostatečném zajištění bezpečnostních opatření se společnost vystavuje riziku, jehož opožděná detekce může způsobovat různé dopady na její fungování. V tomto případě vždy mluvíme o negativních dopadech na společnost. Mezi dopady pro společnost lze zařadit např. finanční ztrátu, ztráta v podobě konkurenčního postavení na trhu, odcizení a zneužití informací, ztráta klíčových informací společnosti, materiální škody, ztráta know-how atd. Rozmanitost dopadů jen potvrzuje závažnost problematiky bezpečnosti informací. V některých případech ovšem nelze úplně tyto hrozby odstranit, nicméně se musíme pokusit o jejich redukci. Zdroj hrozby může být způsoben jak vnitřním, tak vnější faktorem, jejichž nastínění vystihuje následující rozdělení.

Bezpečnostní hrozby lze dělit následujícím způsobem:[39]

- objektivní:
    - přírodní, fyzické jako např. požár, povodeň, výpadek napětí, poruchy apod., u kterých je prevence obtížná a u kterých je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy; v tomto případě je třeba vypravovat havarijní plán;
    - fyzikální např. elektromagnetické vyzařování;
    - technické nebo logické, porucha paměti, softwarová „zadní vrátka“, špatné propojení jinak bezpečných komponent, krádež, resp. zničení paměťového média, nebo nedokonalé zrušení informace na něm;
- subjektivní, tj. hrozby plynoucí z lidského faktoru:
    - neúmyslné, např. působení neškoleného uživatele či správce informačního systému;
    - úmyslné, které je představované potenciální existencí vnějších útočníků, např. špionů, teroristů, kriminálních živlů, konkurentů, hackerů, ale i vnitřních útočníků. Odhaduje se, že 80% útoků na IT je vedeno zevnitř, útočníkem, kterým může být propuštěný zaměstnanec; velmi efektivní z hlediska vedení útoku je součinnost obou typů útočníků.

[39] POŽÁR, Josef, ref. 16.

Základní schéma zajištění bezpečnosti IS a ICT, uvedené na obrázku Obr. 2.12, představuje vztahy mezi aktivy organizace, hrozbami, které na ně mohou potenciálně působit, možnou zranitelností aktiv reálnými hrozbami, dopady reálných hrozeb na tato aktiva a možnostmi ochrany aktiv organizace formou protiopatření.[40]



Obr. 2.12 Schéma zajištění bezpečnosti IS a IT - aktiva a hrozby
Zdroj: POŽÁR, Josef. *Manažerská informatika*. 2010

Poškození či ztráta datových souborů, delší vyřazení systému z provozu, rozšíření počítačových virů v síti nebo průnik do informačního systému je třeba považovat za bezpečnostní incident. Tato událost je vždy provázena informačními ztrátami. Po zjištění bezpečnostního incidentu je třeba vyšetřit jeho příčinu, podrobně analyzovat situaci s cílem zjištění zdrojů infiltrace a uvedení informačního systému do důvěryhodného stavu. Současně s odstraněním důsledků je třeba uskutečnit i opatření zamezující možnosti opakování tohoto jevu. Následující seznam uvádí typické zdroje hrozeb, které mohou přicházet z internetu:[41]

- hackeři, kteří způsobují jen 15-20% prokázaných útoků na internetu;
- snadná možnost odposlechu - napíchnutí (wiretapping) na přenos a zneužití obsahu zprávy;
- krádež identity (Identity Theft) - získání adresy odesílatele, vydávání se za někoho jiného;
- neautorizované programy a možnost jejich modifikace, tzv. cracking;
- distribuce virů a červů;
- odmítnutí služby např. zahlcení elektronickou poštou, kdy je zahlcena služba či disková kapacita;
- dynamická změna hrozeb;
- hoaxy a spamy;

[40] POŽÁR, Josef, ref. 16.
[41] Tamtéž.

- spyware aj.

Ovšem mezi nejzávažnější hrozby informační bezpečnosti můžeme zařadit právě lidský faktor, který je označován jako subjektivní hrozba a stává se často opomíjeným. Každý informační systém i přes implementaci sofistikovaných zabezpečovacích technologií stále může být, díky lidskému faktoru interních zaměstnanců, velice zranitelný. Za lidský faktor lze považovat především činnost uživatelů informačního systému, kdy např. nezkušený uživatel nebyl proškolen v jeho používání a neznalost systému může být kamenem úrazu a svým jednáním může společnosti způsobit značné ztráty a škody. Dále jsou to uživatelé, kterým byl ukončen pracovní poměr v rámci dané společnosti. Tito uživatelé často jednají v afektu a představují hrozbu především ve smyslu úmyslného způsobení škody, jimiž mohou být krádež citlivých informací a jejich zneužití, záměrné zničení dat a informací, vyřazení některých důležitých prvků sítě z provozu, zničení hardwarových součástí apod. V takovém případě je na správci systému či informačním manažerovi stanovit přesná pravidla tak, aby v případě odchodu pracovníka mu byl okamžitě zamezen přístup k informačnímu systému společnosti ještě dřív, než stačí způsobit nějakou škodu a tím takhle předcházet hrozbám tohoto typu. Dalším příkladem jsou uživatelé, jež z nedbalosti a neznalosti mohou útočníkům, pomocí různých metod, umožnit přístup k interním informacím, např. uživatel je vyzván k zadání přístupových údajů do systému na podvodné stránce, otevření infikovaného souboru virem, pomocí kterého útočník získá plnou kontrolu nad počítačem uživatele. Dalším případem může být situace, kdy je uživatelům slíbena odměna za účast ve výzkumu, uživatel přistoupí na spolupráci a poskytne citlivé údaje druhé straně.

Cena utajovaných a před veřejností skrývaných informací šplhá do závratných výšin. Informace se stávají nepřehlédnutelným lákadlem pro konkurenční společnosti i jednotlivce. Výsledky soukromých výzkumů, technické patenty a další jiné utajované informace jsou velmi žádaným zbožím.[42]

2.9 Síťová bezpečnost

Problematika bezpečnosti počítačových sítí je velice rozsáhlá, proto bude tato část zaměřena na definici základních pojmů, které jsou neoddělitelnou součástí síťové bezpečnosti. Síťová

[42] DROZD, Michal. Boj s lidským faktorem v informační bezpečnosti. *IT Systems* [online]. 2007 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/it-security/boj-s-lidskym-faktorem-v-informacni-bezpecnosti.htm

bezpečnost je velice důležitým pojmem, jelikož se čím dál více užívají moderní technologie pracující na principu cloud computingu a využívání virtualizace. A právě otázka síťové bezpečnosti zde působí jako velice zásadní faktor, jehož zabezpečení jej úzce zasahuje.

Bezpečnost definují tři základní charakteristiky (integrita, dostupnost, důvěrnost), přičemž nesplnění jedné z uvedených ohrožuje bezpečnost daného systému. V rámci bezpečnosti obecně musíme mít definované různé druhy bezpečnostních opatření, především tedy organizační (pravidla užívání ICT), technická (dostatečné hardwarové zabezpečení) a fyzická opatření (zamezení přístupu neoprávněných osob k ICT infrastruktuře organizace).

Útoky zaměřené na porušení dostupnosti se nazývají vyřazení z činnosti (Denial of Service). Útoky zaměřené na porušení soukromí nebo integrity jsou v prostředí Internetu většinou klasifikované jako průniky (penetration). Útoky do čtvrté (transportní) úrovně, využívající chyby protokolů, jsou většinou zaměřené jen na vyřazení z činnosti, protože znalostí protokolu vyšší úrovně není možné získat velké výhody. Útoky na protokoly vyšší úrovně (většinou aplikační protokoly) mají charakter průniku, časté jsou však i útoky zaměřené na vyřazení z činnosti. Útoky zaměřené na vyřazení z činnosti (Denial of Service, DoS) mají za cíl zakázat legitimní přístup ke zdroji anebo ke službě. Většinou jsou realizované vyčerpáním veškerých dostupných zdrojů, které jsou zapotřebí k realizaci služby nebo přístupu k ní. Tyto útoky jsou většinou snadno realizovatelné a těžko se jim dá zabránit. Přesto ale nepředstavují vážnou hrozbu. Mezi základní typy útoků patří:[43]

- ICMP bombardování,
- Aplikační útoky,
- SYN záplava,
- Chyby implementací TCP/IP,
- Impersonifikace,
- IP Spoofing,
- Přejmenování stanice,
- Ovlivňování DNS,
- Falšování zpráv elektronické pošty (e-mail forging),
- Drive-by útok atd.

[43] KALETA, Eduard. *Informační technologie: správa počítačových sítí*. 1. vyd. Praha: Professional Publishing, 2008, 180 s. Vzdělávání pro 21. století. ISBN 978-80-86946-61-0.

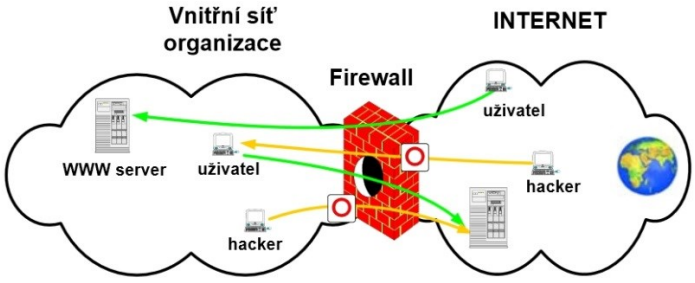
2.10 Obrana proti útokům

Existuje mnoho nástrojů na obranu proti potenciálním bezpečnostním hrozbám, které na uživatele číhají ze všech stran. Avšak řada nástrojů neposkytuje stoprocentní ochranu proti útokům. Slouží pouze jako prevence předcházení nežádoucím jevům, které mohou narušit komunikaci či poškodit uživatelské zařízení. Veškeré incidenty sebou nesou dodatečné náklady pro uživatele na jejich eliminaci či úplné odstranění. Ty základní z nich budou následně popsány.

2.10.1 Firewall a demilitarizovaná zóna

Firewall patří mezi základní formy zabezpečení sítě a jako takový může představovat jak hardwarové, tak softwarové opatření pro zajištění bezpečnosti proti nežádoucím jevům vůči síti. Firewall plní funkci obousměrného zabezpečení, tj. při komunikaci ven ze sítě i při komunikaci směrem do sítě. Během této komunikace zároveň zajišťuje funkci filtru, který dokáže pomocí specifikovaných pravidel rozhodnout o směrování propouštěných paketů.

Firewall odděluje důvěryhodnou a nedůvěryhodnou část sítě, zkoumá datové toky mezi nimi. Firewally se často implementují ne pouze se dvěma rozhraními jako na obrázku Obr. 2.13, ale s dalším třetím rozhraním, ke kterému je připojena tzv. demilitarizovaná zóna (DMZ). V DMZ se typicky vyskytují servery, které mají být přístupny jak z vnitřní sítě, tak z Internetu. Tyto servery mají řádně zabezpečený operační systém, aby nemohlo dojít k jejich napadení. Na servery v DMZ smějí přistupovat jak uživatelé z vnitřní sítě, tak uživatelé z Internetu. Přímý přístup uživatelů z Internetu do vnitřní sítě je však zakázán.[44]



Obr. 2.13 Firewall a jeho funkce

Zdroj: GRYGÁREK, Petr. *Směrované a přepínané sítě* [online], www.vsb.cz

[44] GRYGÁREK, Petr. *Směrované a přepínané sítě* [online]. Ostrava [cit. 2013-04-17]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/bezpecnost-ucitele.pdf. FEI VŠB-TU Ostrava.

Demilitarizovaná zóna se nachází za hlavním směrovačem (routerem), který zajišťuje konektivitu do Internetu, ale zároveň je umístěna před hlavním firewallem. Chráněná podsíť se nachází právě až za hlavním firewallem. Zařízení umístněná v demilitarizované zóně jsou podstatně méně chráněna než zařízení v chráněné podsíti.[45] Další obrázky, znázorňující funkci firewallu i včetně demilitarizované zóny, se nachází v Přílohách 3 a 4.

2.10.2 IDS

Pro detekci útoků a průniků dnes existuje celá řada systému, obecně nazývaná Intrusion Detection Systems (IDS). Tyto systémy neustále sledují provoz na sítí a na základě podezřelých vzorů chování vyhodnocují stavy, které mohou s jistou pravděpodobností indikovat nějaký typ útoku. Vyhledávání provozu indikujícího útok je věcí dosti komplikovanou a může zahrnovat jak různé heuristiky, tak i prvky umělé inteligence. Způsob reakce na oznámené riziko je v IDS již ponechán na administrátorovi. U systému typu IPS (Intrusion Prevention Systems) je automatizace dotažena dále - při vyhodnocení rizika je automaticky provedeno opatření, aby byl další provoz od útočníka odfiltrován. Typicky se jedná o automatickou definici a aplikaci vhodného ACL. Systémy pro detekci a prevenci útoků jsou nezbytné zejména v souvislosti s distribuovanými DoS útoky, u kterých již není v lidských silách dostatečně rychle reagovat na měnící se charakter strojově generovaného útočného provozu a aplikovat příslušná protiopatření.[46]

2.10.3 Antivirový software

Základním krokem úspěšné ochrany výpočetní techniky vyžaduje průběžné aktualizace a jejich součásti ze strany podpory provozovaného operačního systému, které obsahují elementární bezpečnostní nástroje. Ovšem samotný pravidelně aktualizovaný operační systém neposkytuje dostatečné zabezpečení, proto se dodatečně tyto nástroje doplňují o sofistikovanější řešení, pod kterými si lze představit např. antivirové programy, antispyware nástroje, firewally apod. Existuje však i takový software, který obsahuje všechny tyto zmíněné nástroje. U těchto dnes již běžných nástrojů je rovněž zapotřebí udržovat jejich aktuálnost. Cílem antivirového softwaru je včas identifikovat a zastavit činnost nežádoucího a škodlivého softwaru, případně jeho odstranění. To znamená, že takový software pracuje v real-time režimu. Antivirové programy identifikují škodlivý kód na základě virové databáze

[45] HLOBIL, Petr. Bezpečnost počítačových sítí (1): Úvod do problematiky. [online]. 2012 [cit. 2013-04-17]. Dostupné z: http://www.emersion.cz/25744n-bezpecnost-pocitacovych-siti-uvod-do-problematiky
[46] GRYGÁREK, Petr, ref. 44.

(i mimo ni pomocí heuristických algoritmů), která by měla být neustále aktuální díky automatickým aktualizacím, stahovaných ze serveru výrobce. Současné antivirové nástroje mají příjemné a jednoduché uživatelské prostředí, včetně možnosti přepnutí do režimu pro pokročilé uživatele.

Ovšem dokonalého zajištění bezpečnosti počítače nemůžeme nikdy dosáhnout, protože zde opět narážíme na lidský faktor a počínání uživatelů prostřednictvím výpočetní techniky. Každý uživatel by se měl v takovém prostředí chovat vždy s určitou opatrností a zároveň tak, co mu umožňují jeho schopnosti a znalosti. Cílem je aplikovat takové nástroje, které eliminují potenciální hrozby.

V současnosti se v prostředí Internetu vyskytuje poměrně rozsáhlá nabídka komerčních i nekomerčních volně dostupných antivirových SW. Mezi ty nejznámější antivirové nástroje můžeme zmínit např. Avast, AVG, Norton, Microsoft Security Essentials, ESET Smart Security, Kaspersky atd.

2.10.4 Šifrování

Kryptografie poskytuje celou řadu šifrovacích technik k utajení obsahu dat a informací tak, aby byly zabezpečeny při ukládání a přenosu. Šifrování transformuje data takovým způsobem, aby nebyla běžnými prostředky čitelná. V případě odcizení šifrovaných dat nedojde k úniku informací. Šifrování je považováno za nejdokonalejší způsob zabezpečení informací zejména při přenosech pomocí veřejných komunikačních sítí. Přitom se šifrují data při komunikaci, šifrují se data v souborech a discích a používá se digitální podpis. Ten slouží k ověření původu zpráv pomocí elektronického podpisu tak, že je zajištěna nepopiratelnost jména odesílatele zpráv. To znemožňuje zasílání klamných, podvržených a nepravdivých zpráv.[47]

V této souvislosti je třeba zmínit typy šifrovacích mechanismů jakožto základní zabezpečení bezdrátových sítí typu WEP, WPA a WPA2. Přičemž každý má své specifické vlastnosti. Nejméně spolehlivou úrovní zabezpečení je WEP a naopak nejlepším zabezpečením pro bezdrátové sítě je WPA2.

[47] POŽÁR, Josef, ref. 16.

2.10.5 Nevyžádaná pošta - Antispam

V některých publikacích se uvádí, že ze všech příchozích e-mailových zpráv jich více než 70% tvoří spam. Spam neboli výraz označující nevyžádanou poštu, se kterou se setkáváme dnes a denně, byl v dřívějších letech jakýmsi nástrojem, jak obtěžovat uživatele přehlcováním e-mailových schránek a serverů prostřednictvím reklam, klamavých a často nesrozumitelných zpráv apod. V současnosti se jedná o nástroj, ke kterému se přidávají odkazy na nedůvěryhodné a nebezpečné stránky, kde se mohou pro uživatele představovat potenciální hrozby. Prevencí, avšak nikoli dokonalým řešením, proti spamu jsou sofistikované nástroje označované obecně jako antispamový software, jehož hlavním cílem je identifikovat, filtrovat a separovat běžné e-mailové zprávy od podezřelých zpráv, s pokud možno co nejlepším výsledkem. S tímto také souvisí častá implementace algoritmu označovaného jako bayesiánský filtr, který představuje jakýsi expertní systém, jež se neustále učí a na základě získaných znalostí dokáže vyhodnotit a filtrovat příchozí e-maily. Stejně jako u antivirových programů, i antispamové nástroje musíme neustále aktualizovat, aby byla zajištěna jejich aktuálnost a tím i účinnost filtrace zpráv.

2.10.6 VLAN, vzdálený přístup, certifikáty

Virtuální privátní sítě (VPN) jsou mechanismem, umožňující organizacím budovat "privátní" sítě s použitím sdílené infrastruktury, např. veřejného Internetu. Při tom je ale dosaženo stejné úrovně flexibility a bezpečnosti, jako při použití vlastní infrastruktury. Princip VPN spočívá v tunelování šifrovaných dat přes sdílenou infrastrukturu za použití autentizace mezi jednotlivými konci tunelů. Tunelem zde rozumíme virtuální dvoubodové spojení přes sdílenou infrastrukturu, které nese pakety jednoho protokolu zabalené v jiném (nebo i tomtéž) protokolu. Obalujícím protokolem je v Internetu vždy IP, protokolem tunelovaným může být také IP, lze ale přenášet i jiné síťové protokoly (např. Novell IPX) nebo dokonce přímo rámce druhé vrstvy OSI referenčního modelu. Výhodou použití VPN oproti udržování vlastní privátní infrastruktury je nižší cena, flexibilita (virtuální) topologie dána pouze konfigurací firewallů/směrovačů na koncích VPN tunelů. O realizované virtuální topologii nemusí poskytovatel sdílené infrastruktury nic vědět. Také odpadá potřeba dozoru nad vlastními WAN linkami, který je přenechán poskytovateli veřejné infrastruktury.[48]

[48] GRYGÁREK, Petr, ref. 44.

S rozvojem mobilních zařízení a technologií obecně, čím dál více lidí tyto technologie využívá pro účely, kdy se ocitnou mimo organizaci, např. na služební cestě, dovolené či chtějí pracovat z pohodlí domova. Často se stává, že daný zaměstnanec potřebuje vzdáleně přistupovat na pracovní plochu, e-mail či ke konkrétním informacím organizace. Proto je tato možnost dnes běžně využívanou a stala se důležitou součástí, protože umožňuje uživatelům flexibilně pracovat.

2.10.7 Zálohování

Zálohování dat je proces, na který mnoho uživatelů zapomíná. Přitom se vytvoří jedna nebo více kopií požadovaných informací na záložních datových nosičích. V případě zničení či poškození původního media jsou data obnovena ze záložní kopie. Při obnově dat se vždy ta část dat ztratí, která byla vytvořena od posledního zálohování. Platí, že by uživatel měl svá data zálohovat na konci pracovního dne.[49]

Ovšem v dnešní době existují různé zálohovací systémy, které v daných časových intervalech několikrát denně automaticky zálohují práci uživatelů, aniž by oni sami museli tomuto procesu nějak napomáhat. Takové zálohování se provádí zpravidla v několika kopiích za pomoci serverů a externích paměťových zařízení. V případě poruchy či ztráty dat se vyvolá opačný proces, který umožní natáhnutí poslední dostupné verze. Každá organizace by nastavení časových intervalů pro automatické zálohování měla mít nastaveno dle své činnosti a objemu zpracovávaných informací.

[49] POŽÁR, Josef, ref. 16.

3 Průzkum bezpečnosti IS v univerzitním prostředí a analýza výsledků šetření

3.1 Popis univerzitního prostředí

Vysoké školy jsou zvláštním typem organizace, které se vyznačují velkou organizační strukturou, velkým počtem studentů a zaměstnanců (pedagogové, studijní referenti, atd.). V porovnání s podnikatelskou sférou můžeme univerzitní prostředí svým rozsahem a velikostí přirovnat ke korporátní organizaci. Konkrétně VŠB-TU Ostrava navštěvuje 21613 studenů a přibližně 2300 zaměstnanců (z toho 1095 akademických pracovníků)[50]. V současnosti probíhají přípravy na sloučení dvou ostravských univerzit, tedy VŠB-TUO a Ostravskou univerzitou, a díky tomu se zařadit mezi první tři největší univerzity v ČR. Studenty nelze zařadit jako součást personálu univerzity, ale v problematice informační bezpečnosti hrají významnou roli. Je potřeba si uvědomit, že čím větší počet uživatelů takové prostředí obsahuje, tím je obtížnější zajištění veškerých bezpečnostních opatření, kterým musí být věnována důkladná pozornost. Informační technologie jsou nedílnou součástí vybavení škol a studentů, pomocí kterých mohou neustále získávat nové informace. S rozšiřováním informačních technologií dochází k nárůstu přenášených informací, které podléhají bezpečnostním rizikům a vyvolávají potřebu jejich zabezpečení. Dalším charakteristickým prvkem univerzitního prostředí je větší benevolence vůči uživatelům i stanovování politiky IT, než v komerčním prostředí. Už jen z pohledu velikosti univerzitního prostředí, kde se musí ve větší míře aplikovat různá bezpečnostní opatření. Na druhou stranu zde není vyvíjen takový konkurenční tlak na zajištění opatření, jak je tomu u organizací v soukromém sektoru. Důvodem je, že v rámci univerzity se nepracuje s komerčně zajímavými daty, které v podstatě nemají pro potenciální narušitele hodnotu (kromě dat s osobními údaji a hesly uživatelů a výsledků vědecké činnosti).

Například z pohledu bezdrátových technologií, na které musíme pohlížet jako na sdílený prostředek s mnoha každodenními přístupy ze strany uživatelů. Zavedení bezdrátové sítě

[50] VŠB-TU OSTRAVA. *Výroční zpráva o činnosti VŠB - TUO za rok 2011* [online]. Ostrava, 2012 [cit. 2013-04-17]. Dostupné z: http://www.vsb.cz/miranda2/export/sites-root/intranet/innet/cs/okruhy/uredni-deska/vyrocni-zpravy-a-zamery/dokumenty/vz-cinnost-2011.pdf

sebou nese určitá rizika a problémy, které se nemusely nutně řešit v případě klasických sítí. Mezi tyto problémy patří zejména:[51]

- zajištění bezpečné komunikace ve snadno odposlouchavatelném prostředí;
- zajištění autentizace a autorizace uživatelů tak, aby k síti měli přístup pouze oprávnění uživatelé;
- vysledovatelnost různých problémů v tomto dynamicky se měnícím prostředí;
- jednotná metoda přístupu k síti ve všech přístupových bodech sítě;
- co největší interoperabilita.

3.2 Charakteristika VŠB-TU Ostrava

Vysoká škola báňská - Technická univerzita Ostrava patří mezi čtyři největší univerzity v České republice a zároveň zaujímá významné postavení mezi technickými univerzitami ve střední Evropě. VŠB-TU Ostrava se skládá celkově ze sedmi fakult, v rámci kterých nabízí svým uchazečům a studentům obory technického a ekonomického zaměření všech úrovní studia. V roce 2011 bylo na VŠB-TUO zaznamenáno celkem 21613 studentů (z toho 14748 v prezenční formě studia) a 1095 akademických pracovníků[52]. Současným rektorem univerzity je prof. Ing. Ivo Vondrák, CSc. Úplné uspořádání organizační struktury univerzity za rok 2011 je uvedeno v Příloze 7. Univerzita v rámci svého působení rovněž realizuje a účastní se celé řady projektů, včetně současné výstavby významného superpočítačového centra.

Z pohledu informačních technologií má univerzita vlastní celoškolské pracoviště CIT (Centrum informačních technologií), které na univerzitě působí jako hlavní autorita v oblasti IT a počítačových sítí. Oddělení CIT se skládá ze 45 zaměstnanců a disponuje svým vlastním rozpočtem. Úlohou CIT tedy je kompletní správa a rozvoj infrastruktury IT (mimo fakulty) a celouniverzitního informačního systému a zajištění jeho provozu, včetně zajištění a nasazení bezpečnostních opatření. Celouniverzitní informační systém je složen z jednotlivých agend, které pokrývají důležité oblasti fungování univerzity. Přičemž mezi nejzásadnější aplikace využívané uživateli patří zejména pošta, IS Edison, SAP[53], OBD (osobní bibliografická

[51] ROHLEDER, David. Bezdrátové sítě v prostředí MU. *Zpravodaj ÚVT MU* [online]. 2004, XIV, č. 3 [cit. 2013-04-17]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/clanky_tisk/297.pdf

[52] Číselné údaje byly použity z Výroční zprávy o činnosti VŠB-TU Ostrava za rok 2011, ref.

[53] SAP je komplexní podnikový informační systém typu ERP (Enterprise Resource Planning), který lze díky své modularitě přizpůsobit podle potřeb organizace. SAP se skládá z množství agend, které pokrývají různé procesy spojené s fungováním organizace. Pomocí SAP lze zpracovávat data v oblasti např. účetnictví, prodeje a fakturace, výroby, logisticky, controllingu apod.

databáze) a intranet (InNET) apod. Kompletní informační systém a jeho části jsou zachyceny v tabulce Přílohy 6. V oblasti informační bezpečnosti, CIT provádí veškeré činnosti v souladu s normou ISO/IEC 27001. V rámci útvaru CIT je také Helpdeskové pracoviště, které poskytuje podporu všem uživatelům univerzity a řeší problémy a požadavky vzešlé ze strany uživatelů.

CSIRT (Computer Security Incident Response Team) tým je pracovní skupina zabývající se zpracováním bezpečnostních incidentů v oblasti informačních technologií. CSIRT tým je složen z pracovníků oddělení CIT - infrastruktura a je oprávněn provádět takové technické kroky, které umožňují aktivně vyhledávat ty stanice v síti VŠB-TUO, které jsou napadeny, poskytují data v rozporu se zákony ČR, jsou zneužívány nebo obsahují takové programové vybavení, které je možno neoprávněně využít bez vědomí správce nebo uživatele síťového prostředku.[54]

3.3 Charakteristika univerzitní sítě

V rámci univerzitní sítě a infrastruktury se klade důraz na zpřístupnění Internetu a jeho zajištění pro co největší počet studentů i zaměstnanců ve všech prostorech a budovách univerzity, které jsou uživatelům přístupné. Toho lze docílit pomocí instalace klasických zásuvkových přípojek nebo prostřednictvím efektivnějšího přístupu bezdrátových sítí. V případě bezdrátových sítí se nabízí uživatelům jiná možnost práce, kdy např. studenti pracují na kolektivní práci na jakémkoliv místě univerzity, během které se neobejdou bez neustálého připojení k Internetu. Tato možnost zpřístupnění Internetu je uživateli (studenty i zaměstnanci) velice oblíbená a hojně využívána, a zajišťuje jim flexibilitu při řešení různých problémů. Dá se říct, že uživatelé dnes považují možnost připojení do sítě Internet za automatickou, kdekoliv se pohybují. A to i díky dostupnosti zařízení typu notebook, tablet či smartphone, které se v současnosti považují za běžné součásti každého studenta. Cílem implementace bezdrátových sítí je i zajištění dostatečného signálu pro připojení k přístupovému bodu a jeho pokrytí v pokud možno co největším počtu přístupných míst. V každém případě je nutné se do sítě autentizovat pomocí jedinečného identifikátoru (např. osobního čísla) a hesla, které jsou uživateli přiděleny při navázání vztahu s univerzitou. Navázáním vztahu s univerzitou můžeme rozumět úspěšné přijetí studenta ke studiu, přijetí

[54] TUO_SME_09_001. *Řešení bezpečnostních IT incidentů na VŠB-TU Ostrava*. Ostrava: VŠB-TUO, 2009. Dostupné z: https://www.vsb.cz/share/uploadedfiles/secured/smernice/SME_09_001.pdf

zaměstnance do personálu univerzity, přijetí nového akademického pracovníka apod. Úspěšným zadáním údajů je uživateli umožněn přístup do sítě Internet.

V rámci sdružení počítačových sítí CESNET je v České republice realizován projekt akademického roamingového systému **eduroam**[55] (zkratka EDUcation ROAMing), do kterého jsou zapojeny téměř všechny veřejné vysoké školy a Akademie věd ČR (celkem 27 členských institucí[56]). Cílem projektu je zajistit síťovou konektivitu mezi jednotlivými sítěmi vysokých škol, které jsou do tohoto systému zapojeny, i v rámci celé Evropy. Motivací všech prací je, aby použití služeb sítě bylo tak snadné, jako je používání roamingu mobilních operátorů. Uživatel má jediný účet (ve své domovské síti) a tento účet jej opravňuje k použití bezdrátové sítě kteréhokoliv člena projektu.[57]

Sdružení CESNET založily vysoké školy a Akademie věd České republiky v roce 1996. Jeho hlavním cílem je výzkum a vývoj informačních a komunikačních technologií, budování a rozvoj e-infrastruktury CESNET určené pro výzkum a vzdělávání. Zkratka CESNET znamená Czech Education and Scientific NETwork.[58]

Síť zajišťující roaming můžeme definovat jako připojení na Internet, které je funkční i při pohybu koncového zařízení (notebook, tablet, atd.) jak v rámci jednoho přístupového bodu, tak i při pohybu mezi nimi. Je tedy možno se připojit jak mezi jednotlivými budovami, tak např. bezprostředně po vstupu do budovy a pak se po ní volně pohybovat, aniž by došlo ke ztrátě spojení či změně jeho parametrů (např. IP adresa zařízení).[59]

3.3.1 Univerzitní síť VŠB-TU Ostrava

Infrastruktura univerzity poskytuje uživatelům možnost připojení do sítě Internet prostřednictvím speciálně vyhrazených prostor (počítačové učebny) a bezdrátového připojení. Jelikož je i VŠB-TU Ostrava zapojena do projektu eduroam, umožňuje uživatelům volný pohyb díky jeho dostupnosti. Uživatelům, tedy zaměstnancům a především studentům, je připojení pomocí svého zařízení k Internetu umožněno na základě přihlašovacích údajů.

[55] Název a logo eduroam jsou registrovanou ochrannou známkou společnosti TERENA (Trans-European Research and Educational Networking Association).
[56] CESNET. *CESNET* [online]. 2013 [cit. 2013-04-17]. Dostupné z: http://www.cesnet.cz/sdruzeni/
[57] EDUROAM. *Eduroam.cz* [online]. 2012 [cit. 2013-04-17]. Dostupné z: http://www.eduroam.cz/
[58] CESNET, ref. 56.
[59] MATYSKA, Luděk. Bezdrátová síť Fakulty informatiky. *Zpravodaj ÚVT MU* [online]. 2002, XII, č. 3 [cit. 2013-04-17]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/clanky_tisk/236.pdf

Přihlašovací údaje studentů a zaměstnanců tvoří unikátní univerzitní kód a heslo, které jsou jim přiděleny. To znamená, že bezdrátová síť je dostupná i uživatelům, kteří nejsou přímo spojeni s danou univerzitou, ale spadají pod jinou instituci, účastnící se projektu eduroam. Proto si každý uživatel z jiné univerzity musí nejdříve ověřit, zda se jeho kmenová univerzita účastní projektu eduroam. Na serveru eduroam.cz lze nalézt mapu všech eduroam institucí. Vzhledem k různě situovaným fakultám VŠB-TU Ostrava, eduroam pracuje na všech těchto místech, včetně ubytovacích zařízeních. Zároveň by studenti i zaměstnanci neměli mít problém s připojením i na Ostravské univerzitě, která je také součástí projektu eduroam.

Interní uživatelé mohou také využívat přístupu k vnitřní síti univerzity prostřednictvím služby VPN, za pomoci potřebného klienta. To umožňuje uživatelům využívat např. služeb serverů a nemusí si tak instalovat sofistikované a mnohdy nákladné nástroje na vlastní zařízení. Pro připojení přes VPN se uživatel nesmí se svým připojeným zařízením pohybovat v rámci univerzitní sítě. Musí se tedy nacházet mimo univerzitní síť. Uživatelé, kteří chtějí využívat daných služeb a nachází se uvnitř lokální sítě, k přístupu nepotřebují VPN klienta.

3.3.2 Další typy sítí VŠB-TUO

Bezdrátová síť **tuonet-peap-5g** je dostupná pouze ve frekvenčním pásmu 5GHz (méně zarušené pásmo poskytující vyšší kvalitu/rychlost připojení) a je k dispozici u většiny přístupových bodů v areálu Poruba, zejména pak přednáškové sály a foyer, tedy místa s velkým počtem připojených klientů. Svojí konfigurací je, vyjma názvu, shodná se sítí tuonet-peap. Tato síť umožňuje bezdrátové připojení jak na VŠB-TUO, tak i v bezdrátových sítích jiných akademických institucí zapojených do mezinárodního projektu eduroam. Návštěvám z těchto akademických institucí pak umožňuje připojení na VŠB-TUO.[60]

Síť **tuonet-simple** určená pro koncová zařízení (např. PDA, MDA), která nepodporují žádné autentizační a šifrovací mechanismy, popř. jsou s nimi technické problémy. Avšak používání této sítě není zcela bezpečné, protože radiový signál, který šíří přístupové body se volně šíří prostorem a je možné jej zachytit kdekoliv v dosahu přístupového bodu. Na rozdíl od "drátové" sítě může prakticky kdokoliv s notebookem a speciálním programovým vybavením komunikaci na síti monitorovat.[61]

[60] VŠB-TU OSTRAVA. *WIFI - Bezdrátová síť VŠB-TU Ostrava* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/sluzby/wifi/
[61] Tamtéž.

3.3.3 Bezpečnostní opatření VŠB-TUO

V rámci síťové infrastruktury musí správci IT řešit neustálé monitorování sítě a s ní spojenou klasifikaci bezpečnostních rizik. Problémem, který s poskytováním Internetu přímo souvisí, je otázka přenášených informací a jejich zabezpečení před nežádoucími jevy v síti. Proto hlavním cílem zabezpečení informací je zajištění třech hlavních cílů informační bezpečnosti, tj. důvěrnost, integrita a dostupnost těchto informací. Takovým opatřením může být např. využívání šifrované komunikace, šifrování dat samotných, nastavení přístupových práv uživatelům atd. Opět v případě bezdrátových sítí, k nimž se může kdokoliv přistupovat, hrozí odposlech komunikace v síti, k jehož zachycení dnes není zapotřebí speciálních zařízení.

Všechny části sítě TUONET jsou před viry a útoky z Internetu zabezpečeny pomocí specializovaných zařízení. Tato zařízení plní funkci síťového antiviru, který scanuje HTTP, FTP, POP3 a IMAP provoz. Dále fungují jako IPS (Intrusion Protection System), který prohlíží procházející provoz, a pokud v něm nalezne signaturu známého útoku nebo škodlivého kódu, zaznamená varovnou zprávu a případně podezřelý provoz zablokuje. Také je schopno provádět detekci anomálií v síťovém provozu, například extrémně vysoký počet spojení z jednoho počítače, který může být způsoben šířením červa. Konkrétně se používá několik různých typů zařízení Fortigate firmy Fortinet. Na základě informací získaných systémem IPS jsou od školní sítě odpojovány zavirované nebo jinak napadené počítače. Uživatelé jsou o tom informováni prostřednictvím stránky v interním systému univerzity nebo univerzitním e-mailem. Do seznamu blokovaných počítačů se automaticky přidávají počítače, které byly zablokovány z důvodu napadení malwarem nebo na nich docházelo k porušování pravidel pro připojení k síti TUONET.[62]

Konkrétně síť **eduroam** je k dispozici na všech bezdrátových přístupových bodech sítě univerzity a u této sítě se používá šifrování WPA2 + AES / WPA + TKIP. Ze sítě eduroam rovněž není povolen provoz protokolu SMTP, blokován je port TCP/25.[63]

Aby byl minimalizován počet incidentů v počítačové síti, probíhá v počítačové síti monitoring následujících informací:[64]

[62] VŠB-TU OSTRAVA. *Antivirová ochrana a IPS* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/sluzby/IPS/

[63] VŠB-TU OSTRAVA. *Eduroam - návštěvy na VŠB-TU Ostrava* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/sluzby/eduroam/visitors/

[64] VŠB-TU OSTRAVA. *Autorský zákon a počítačová síť VŠB-TU Ostrava* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/pravidla/az/

- měření množství přenesených dat jednotlivých koncových stanic studentů i zaměstnanců;
- zjišťování, zda koncová stanice používá aplikace pro sdílení dat v počítačové síti.

Uživatelé sítě v rámci univerzity se musí během své práce v této síti řídit danými směrnicemi, pravidly a provozními řády. Tato pravidla jsou umístěna v dokumentačním systému univerzity a jsou veřejně dostupná každému uživateli. Zároveň musí každý uživatel jednat v souladu s autorským zákonem. Uživatel nesmí sdílet takový obsah, ke kterému nemá licenci či autorská práva. V případě porušení autorských práv musí univerzita poskytnout údaje o uživateli a spolupracovat ve vyšetřování. Stejně tak v tomto případě musí uživatel podat vysvětlení správci počítačové sítě.

Pokud je zjištěno, že z koncové stanice proudí do Internetu velké množství dat a zároveň stanice používá některou z výměnných sítí, pak je uživateli zaslán e-mail s žádostí o vysvětlení. Po uživateli stanice (popř. po příslušném správci) je požadováno vysvětlení nadměrného přenosu dat a ověření technického stavu, ve kterém se stanice nachází (např. není-li zavirována nebo jinak zneužívána jinou osobou než oprávněným uživatelem). Veškeré incidenty jsou dokumentovány. Dokumentovány jsou také jednotlivé úkony technických pracovníků i uživatelů při řešení incidentu. Provoz koncových stanic nebo uživatelů může být omezen nebo zcela znemožněn a to až do doby úplného vyřešení problému.[65]

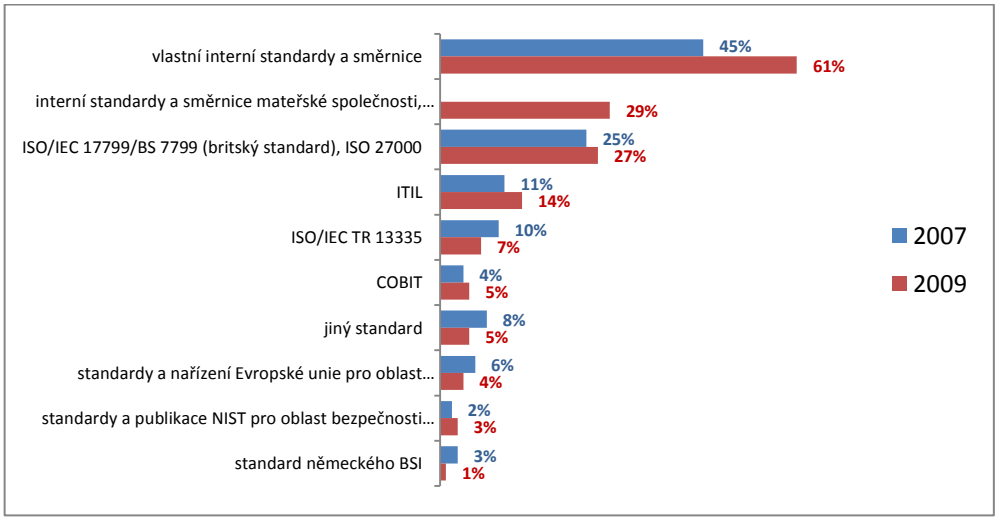
Uživatelé musí mít na paměti, že mnohé klientské programy výměnných sítí umožňují data nejen stahovat, ale také nabízet a to i ve chvíli, kdy je stažena jen část těchto dat. Už v této chvíli tak může uživatel porušovat autorský zákon. Proto je doporučováno, aby uživatelé používali výměnné sítě na výměnu pouze těch dat, k nimž mají autorská práva, popř. licence umožňuje tato data nabízet dalším uživatelům počítačové sítě. Policie ČR je v této oblasti v současné době poměrně aktivní a i na VŠB-TUO přicházejí žádosti o poskytnutí údajů o uživatelích koncových stanic. Uživatelé se sami protizákonným jednáním vystavují trestněprávnímu postihu.[66]

[65] VŠB-TU OSTRAVA, ref. 64.
[66] Tamtéž.

3.4 Průzkum stavu informační bezpečnosti

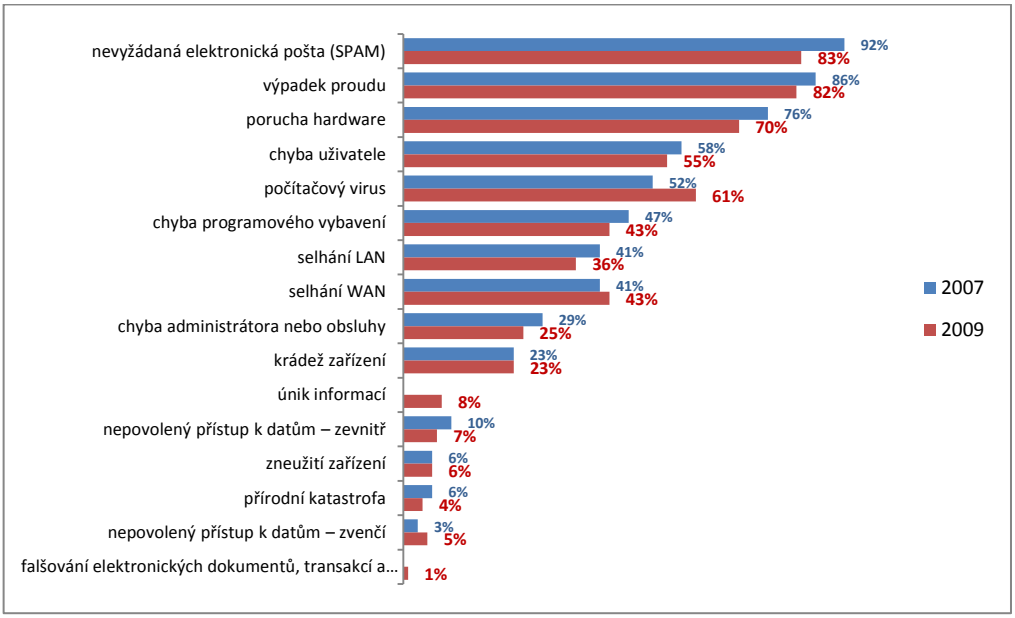
Tato část práce se bude věnovat konkrétním již realizovaným výzkumům v oblasti informačního zabezpečení. V této problematice je důležité zmínit dva významné průzkumy zaměřené na úroveň zabezpečení informací organizací. První rozsáhlý průzkum PSIB je výsledkem společné práce partnerů Ernst & Young, Národního bezpečnostního úřad (NBÚ) a časopisu DSM (Data Security Management), jehož cílovou skupinou respondentů byli organizace soukromého sektoru. Druhým průzkumem je projekt realizovaný na VŠB-TU Ostrava, avšak se zaměřením na úroveň zajištění bezpečnosti informací v rámci veřejných i soukromých vysokých škol. Poté bude následovat stěžejní část této diplomové práce, jež bude obsahovat rozbor a popis výsledků získaných z dotazníkového šetření, které probíhalo pouze v prostředí VŠB-TU Ostrava.

První ročník průzkumu stavu informační bezpečnosti v ČR (PSIB), jehož partnery jsou Ernst & Young, NBÚ a časopis DSM, pochází z roku 1999. Tento průzkum se zabývá širokým spektrem otázek v oblasti informační bezpečnosti, mezi něž patří např. otázky bezpečnostní politiky, standardů, hodnocení informační bezpečnosti a její organizační zajištění a řešení atd. Průzkum probíhal v ČR každé dva roky, prozatím poslední ročník PSIB pochází z roku 2009 a zaměřuje se na monitorování stavu a vnímání informační bezpečnosti v komerčním sektoru. Pro názorné srovnání byly vybrány pouze některé důležité oblasti, které jsou popisovány v této práci. Přičemž nejzajímavějším ukazatelem je otázka implementace některého ze standardů v prostředí českých firem a přehled nejčastějších bezpečnostních incidentů.



Graf 3.1 Využívání standardů v oblasti informační bezpečnosti z průzkumů PSIB 2007 a 2009
Zdroj: DSM. Průzkum stavu informační bezpečnosti [online], www.tate.cz; vlastní tvorba

Z grafu si lze všimnout, že většina organizací stále uplatňuje vlastní definované standardy a směrnice, takto odpovědělo 61% respondentů. Následuje řízení IT pomocí interních standardů, které jsou převzaty od mateřské společnosti. Dalším zajímavým výsledkem je využívání norem řady ISO 27000 (ISO/IEC 17799 a BS 7799 jsou předchůdci této normy) a rámce ITIL, u nichž došlo oproti minulému ročníku průzkumu z roku 2007 k mírnému nárůstu.



Graf 3.2 Výskyt bezpečnostních incidentů z průzkumů PSIB 2007 a 2009
Zdroj: DSM. Průzkum stavu informační bezpečnosti [online], www.tate.cz; vlastní tvorba

Nejčastěji vyskytované bezpečnostní incidenty způsobují z 83% SPAMy, tedy nevyžádaná pošta, která zaplavuje schránky uživatelů. Avšak oproti ročníku z roku 2007 tento ukazatel klesl o téměř 10 procentních bodů. Mezi další nejčastější bezpečnostní incidenty, se kterými se firmy potýkají, patří výpadek proudu (82%), porucha hardwarových komponent (70%), počítačový virus (61%) nebo chyba uživatelů (55%). U těchto hlavních uvedených výsledků, kromě počítačových virů, došlo k mírnému poklesu, naopak se vyskytl opětovný problém s počítačovými viry, u nichž byla změna v podobě nárůstu o téměř 10% oproti roku 2007.

3.5 Dotazník informační bezpečnosti na univerzitě

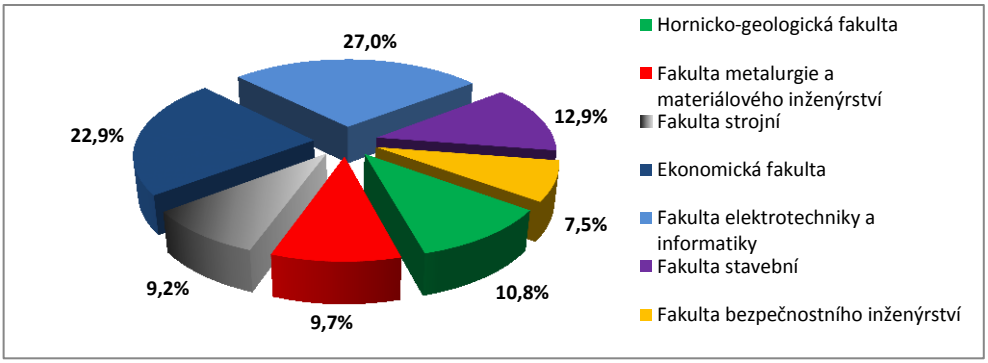
V rámci mé diplomové práce byl na univerzitě VŠB-TU Ostrava realizován průzkum pomocí dotazníkové metody. Tento průzkum se zaměřuje na problematiku informační bezpečnosti v univerzitním prostředí VŠB-TUO a navazuje na projekt realizovaný v roce 2011, který se

zabýval úrovní informační bezpečnosti na univerzitách v České republice, avšak z pohledu jednotlivých zaměstnanců zodpovědných za oblast informační bezpečnosti. Z tohoto důvodu lze následující dotazník chápat jako doplňující materiál zaměřující se na užší komunitu, tvořenou studenty univerzity VŠB-TUO. Studenti tvoří důležitou součást v oblasti informační bezpečnosti univerzity. Jednotlivé otázky jsou záměrně strukturovány tak, aby dotazník na respondenta působil jednoduše a jeho vyplňování mu nečinilo problémy. I proto musely být odpovědi jednotlivých otázek formulovány jednoznačným (uzavřeným) výčtem odpovědí nebo číselnou stupnicí a neumožnovali tak respondentům volné textové odpovědi.

Cílem průzkumu je získání informací z řad studentů univerzity o jejich přístupu a vnímání informační bezpečnosti na univerzitě, a zároveň zjistit jejich preference v této oblasti. Dotazník byl mezi studenty publikován a distribuován v elektronické podobě prostřednictvím sociálních skupin, zaměřených pro studijní účely daných fakult. Z mnoha dostupných prostředí pro sestavení dotazníku byla vybrána bezplatná služba Google Drive, která nabízí předpřipravené formuláře vhodné pro vytváření dotazníků. Během tří týdenního šetření byli osloveni studenti všech fakult univerzity, a celkově bylo zaznamenáno 371 odpovědí. Dotazník v celé své podobě je obsažen v Příloze 5. Získané výsledky dotazníku pomohou pracovníkům CIT při řešení slabých míst v problematice informační bezpečnosti univerzity.

Otázka č. 1 - Jakou fakultu navštěvujete v rámci studia na VŠB-TU Ostrava?

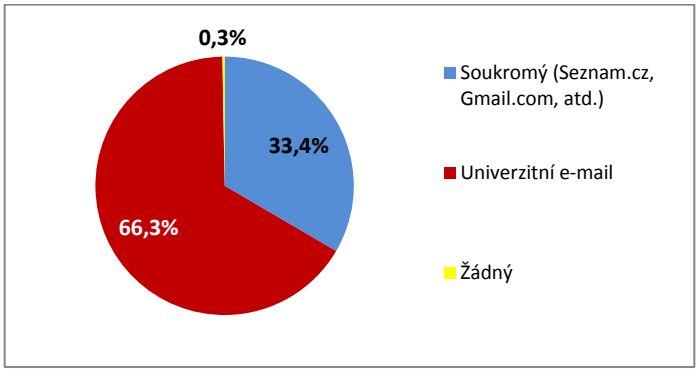
Odpovědi týkající se kmenových fakult studentů jsou takřka ve stejném poměru, s výjimkou fakult elektrotechniky a informatiky a ekonomické. U ekonomické fakulty tomuto výsledku (téměř 23%) může nahrávat fakt, že je fakultou s největším počtem studentů z VŠB-TUO. Nejvíce odpovídali studenti informatiky a elektrotechniky (27%), což může hrát ve výsledcích dotazníku určitou roli. Od těchto studentů se očekává, že problematiku informační bezpečnosti znají a je jim blízká, což jen přidává na relevantnosti dosažených výsledků.



Graf 3.3 Jakou fakultu navštěvujete v rámci studia na VŠB-TU Ostrava?; vlastní zpracování

Otázka č. 2 - Jaký e-mail převážně využíváte ke komunikaci např. s pedagogem, zaměstnanci univerzity?

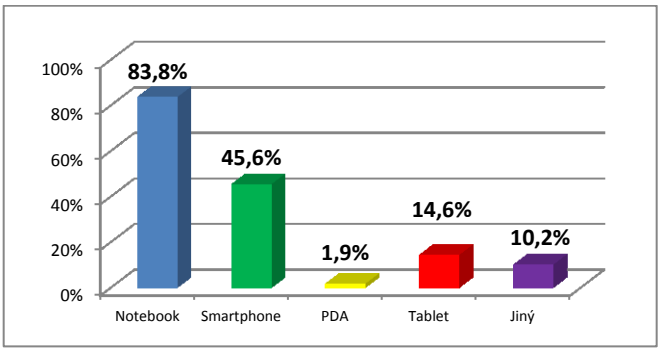
Většina respondentů, celkově 66% studentů, využívá ke komunikaci univerzitní e-mail, což je trochu překvapující výsledek. Soukromý e-mail, u kterého bylo očekávání považováno za preferovanější formu komunikace před univerzitním e-mailem, využívá 33% dotázaných.



Graf 3.4 Jaký e-mail převážně využíváte ke komunikaci např. s pedagogem, zaměstnanci univerzity?; vlastní zpracování

Otázka č. 3 - Jakým zařízením se připojujete k univerzitní bezdrátové síti?

Zde studenti mohli označit více možností a z uvedených výsledků se názorně potvrzuje rychle rostoucí trend využívání chytrých telefonů (46%) a tabletů (15%). Ovšem nejvyužívanějším zařízením stále dominuje notebook, se kterým pracuje téměř 84% uživatelů. Pod jiným zařízením si lze představit čtečky elektronických knih či PlayStation Portable apod., které rovněž podporují připojení k bezdrátové síti.

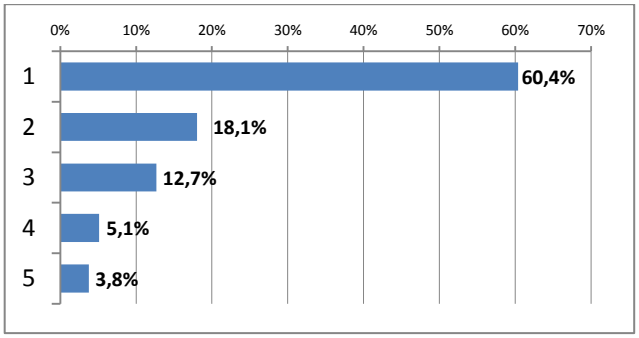


Graf 3.5 Jakým zařízením se připojujete k univerzitní bezdrátové síti?; vlastní zpracování

Otázka č. 4 - Jakým způsobem je pro Vás zásadní bezdrátové připojení na univerzitě?

V dnešní době berou studenti bezdrátové připojení jako automatickou součást svého studia na vysoké škole, o čemž také vypovídá výsledek průzkumu. Z nabízené stupnice, kdy 1 znamená

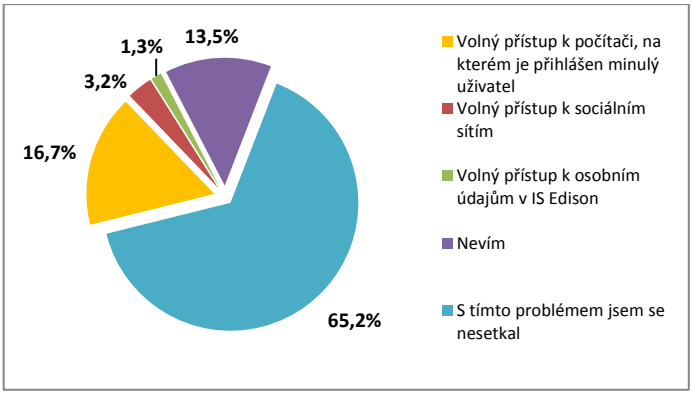
důležité a 5 *nepoužívám*, nadpoloviční většina (60%) označila, že možnost bezdrátového připojení v rámci univerzity je pro ně důležité.



Graf 3.6 Jakým způsobem je pro Vás zásadní bezdrátové připojení na univerzitě?; vlastní zpracování

Otázka č. 5 - Setkali jste se s problémem zneužití osobních údajů na univerzitě?

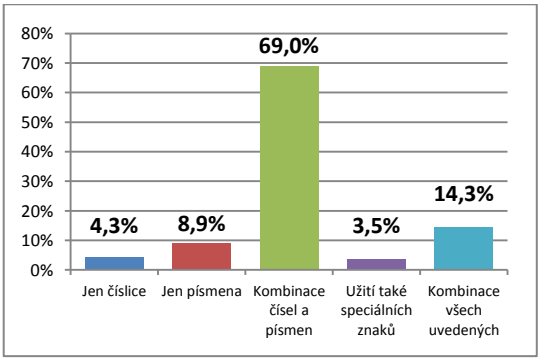
Otázka sleduje, zda se studentům přihodila situace, kdy po vstupu do učebny usedli k počítači, na kterém byl přihlášený předchozí uživatel. Může se stát, že na stanici zůstala otevřená relace některé z webových služeb (např. Edison, Facebook, Twitter apod.). Nebo uživatel sám byl obětí zneužití informací, protože nedopatřením zapomněl zavřít všechny využívané služby či vypnutím počítače ukončit veškerou svou činnost. Z výsledků vyplývá, že téměř 17% uživatelů mělo volný přístup k počítači, na kterém byl přihlášen předchozí uživatel. Někteří se setkali i s otevřenou relací na sociálních sítích a IS Edison. Avšak podstatné je, že většina uživatelů (65%) se s tímto problém nesetkalo, anebo o něm neví (13%).



Graf 3.7 Setkali jste se s problémem zneužití osobních údajů na univerzitě?; vlastní zpracování

Otázka č. 6 - Jaká upřednostňujete hesla pro přihlašování do různých systémů univerzity?

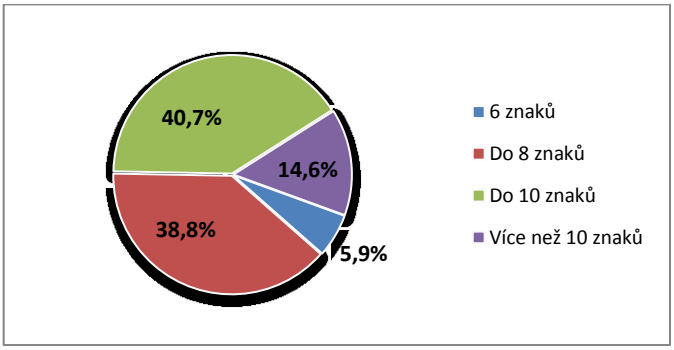
Z výsledků je jednoznačné, že studenti nejčastěji pro svá hesla volí kombinaci čísel a písmen. Takto odpovědělo 69% respondentů. Následuje menší část studentů (14%), kteří v rámci volby svých hesel kombinují všechny možnosti, tedy číslice, písmena i speciální znaky. Z pohledu bezpečnosti informací se tyto dvě kombinace považují za jedny z nejsilnějších a nejúčinnějších. Útočníci využívají speciální algoritmy na dešifrování hesel, a tyto kombinace hesel je velice náročné odhalit.



Graf 3.8 Jaká upřednostňujete hesla pro přihlašování do různých systémů univerzity?; vlastní zpracování

Otázka č. 7 - Jaká je podle Vás ideální délka hesla pro vstup do jednotlivých systémů?

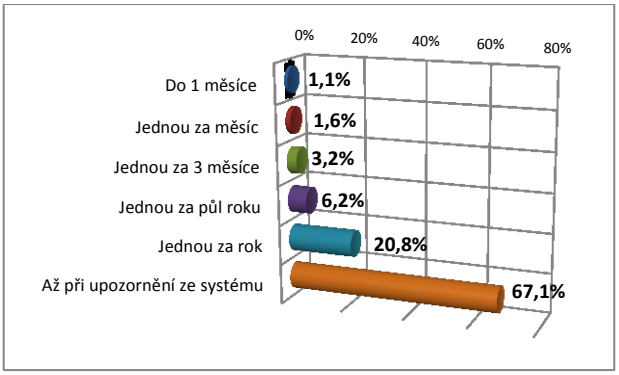
Problematika s typem kombinace hesla úzce souvisí s jeho délkou. Samozřejmě platí, že čím větší délka hesla je, tím je opět pro útočníky obtížnější takové heslo odhalit. Doporučená délka hesla z hlediska bezpečnosti se vždy různí, ale takový optimální střed je min. osm znaků. Z odpovědí vyplývá, že nejčastěji uživatelé volí svou délku do osmi či deseti znaků. Téměř 15% respondentů využívá heslo delší než deset znaků.



Graf 3.9 Jaká je podle Vás ideální délka hesla pro vstup do jednotlivých systémů?; vlastní zpracování

Otázka č. 8 - Jak často si měníte heslo pro přístup do univerzitního systému?

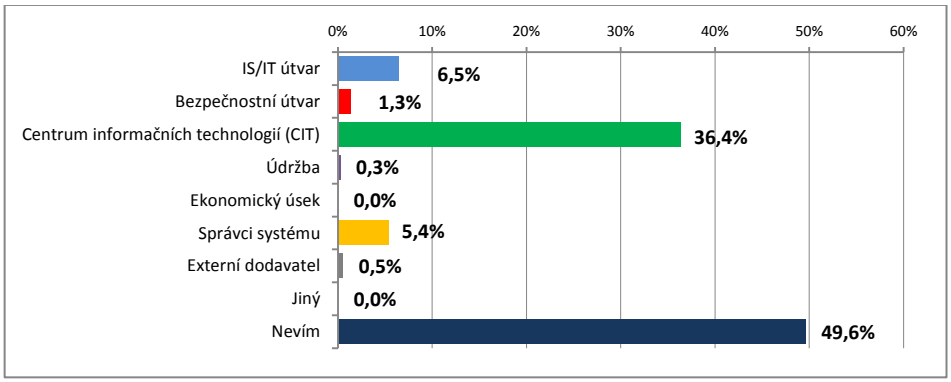
Cílem této otázky bylo zjistit, zda si uživatelé mění své heslo pro přístup do univerzitního systému sami, nebo tomuto problému nechávají volný průběh a učiní tak až při obdržení varovné zprávy. Očekávání se však naplnilo a nadpoloviční většina si mění heslo, až když jsou vyzváni ze strany systému prostřednictvím e-mailu. Téměř 20% uživatelů si mění své heslo sami nezávisle na systému.



Graf 3.10 Jak často si měníte heslo pro přístup do univerzitního systému?; vlastní zpracování

Otázka č. 9 - Víte, který útvar univerzity se stará o informační bezpečnost v rámci univerzity?

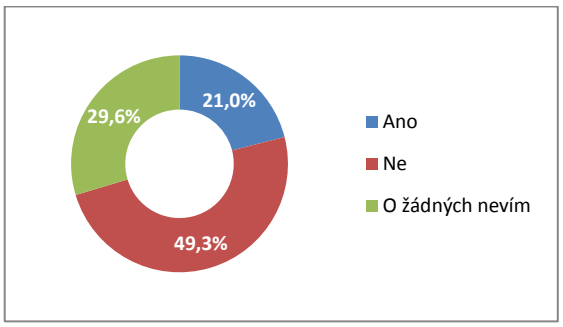
Otázka sleduje informovanost a orientaci studentů, jestli mají tušení o tom, kdo je zodpovědný o správu infrastruktury IT a zajištění její bezpečnosti. Překvapivě skoro 50% studentů neví, který útvar univerzity se problematikou informační bezpečnosti zabývá. Naopak 36% studentů reagovalo správně, že oblast informační bezpečnosti univerzity má pod správou oddělení Centrum informačních technologií (CIT).



Graf 3.11 Víte, který útvar univerzity se stará o informační bezpečnost v rámci univerzity?; vlastní zpracování

Otázka č. 10 - Seznámili jste se se směrnicemi a provozními řády týkajících se informační bezpečnosti v rámci univerzity?

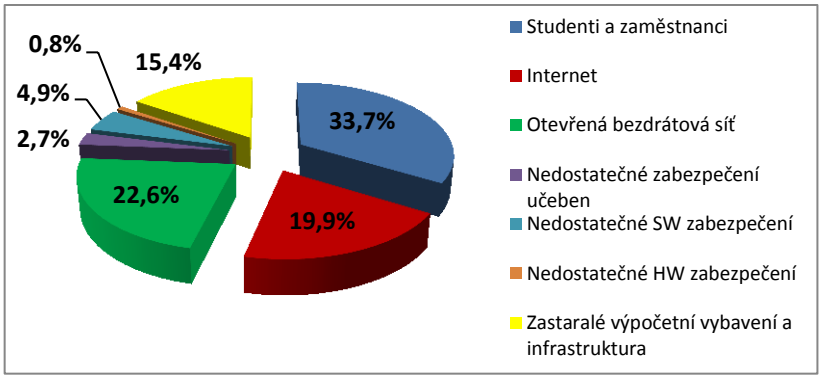
V oblasti pravidel a směrnic, týkajících se informační bezpečnost, skoro polovina z dotázaných se doposud neseznámila se směrnicemi. Dalších 30% dokonce neví o tom, že takové informace existují a neví, kde se nachází. Pouhých 21% studentů věnovalo této problematice pozornost. Studenti mohou veškeré směrnice a řády najít v dokumentačním systému univerzity.



Graf 3.12 Seznámili jste se se směrnicemi a provozními řády týkajících se informační bezpečnosti v rámci univerzity?; vlastní zpracování

Otázka č. 11 - Co pro Vás představuje největší hrozbu z hlediska informační bezpečnosti na univerzitě?

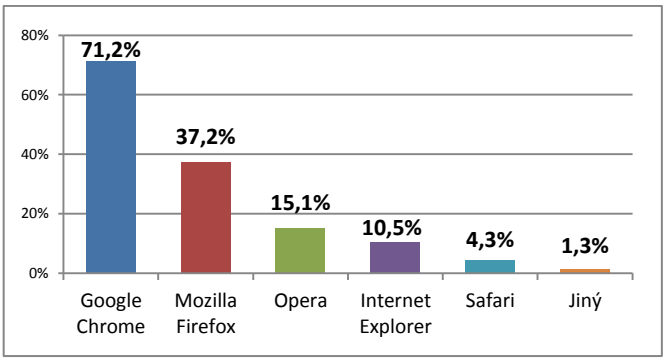
Otázka zjišťuje, jak jsou bezpečnostní hrozby vnímány samotnými studenty a co podle nich představuje největší bezpečnostní hrozbu pro uživatele a univerzitní síť všeobecně. Z následujících odpovědí si lze všimnout, že nejvíce studentů (34%) za největší hrozbu považuje lidský faktor, tedy studenty a zaměstnance. Další potenciální hrozby podle studentů mohou pocházet z bezdrátové sítě (odposlech komunikace apod.). Pak je to internet samotný, za kterým se skrývá mnoho nástrah na uživatele. Významný počet studentů vnímá jako hrozbu i zastaralé vybavení výpočetní techniky.



Graf 3.13 Co pro Vás představuje největší hrozbu z hlediska informační bezpečnosti na univerzitě?; vlastní zpracování

Otázka č. 12 - Jaký internetový prohlížeč používáte pro prohlížení webových stránek?

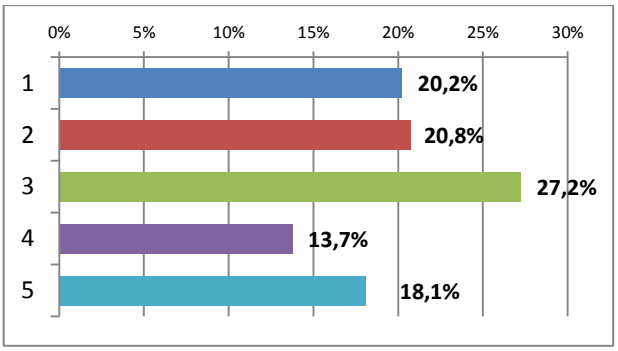
Pro bezpečné procházení internetu je nutné být vybaven i vhodným internetovým prohlížečem, ve kterých jsou aplikovány nástroje pro obranu před bezpečnostními hrozbami. Jednotlivé prohlížeče jsou každoročně poměřovány a podstupují testy zaměřující se na bezpečnost uživatele. Zde měli studenti možnost označit více variant, protože v případě nahodilých problémů s webovým obsahem většinou volí alternativní prohlížeč. Odpovědi zároveň mohou vypovídat o preferencích uživatelů, jaký internetový prohlížeč považují za nejbezpečnější. Studenti jako nejvíce preferovaný prohlížet označili Google Chrome, poté je to Mozilla Firefox a Opera. To, jak si stojí jednotlivé prohlížeče v současných verzích, ukazuje test, obsažený v jiné časti této práce.



Graf 3.14 Jaký internetový prohlížeč používáte pro prohlížení webových stránek?; vlastní zpracování

Otázka č. 13 - Jak významná je pro Vás možnost vzdáleného přístupu z domova do univerzitní sítě, např. pomocí VPN?

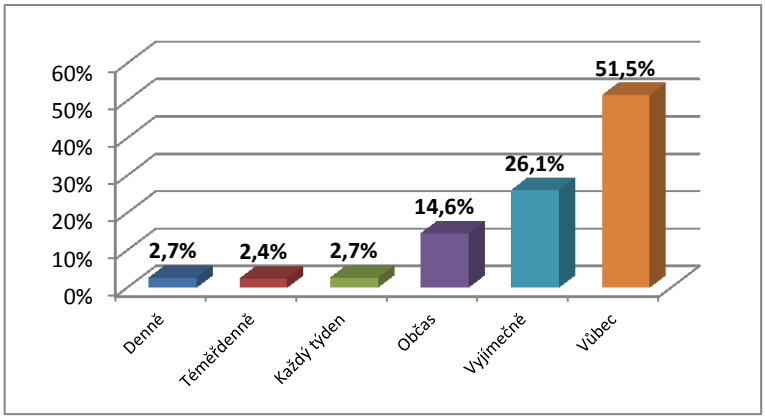
Studentům je umožněno v rámci zpracování různých projektů přístup do interní sítě univerzity prostřednictvím VPN služby. To sebou nese určitá rizika během výměny dat, proto cílem této otázky bylo zjistit využívání služby VPN z řad studentů. Odpovědi byli ve formě stupnice od 1 do 5 (1 - významná, 5 - nevýznamná). Odpovědi byly poměrně vyrovnané, přičemž nejvíce odpovědí bylo zaznamenáno s možností 3, značící neurčitý postoj respondentů k využívání této služby. Ale lze konstatovat, že pro 41% studentů je možnost využití VPN významná.



Graf 3.15 Jak významná je pro Vás možnost vzdáleného přístupu z domova do univerzitní sítě, např. pomocí VPN?; vlastní zpracování

Otázka č. 14 - Jak často se setkáváte s problémem nevyžádané pošty (tzv. Spam) na Vašem univerzitním e-mailu?

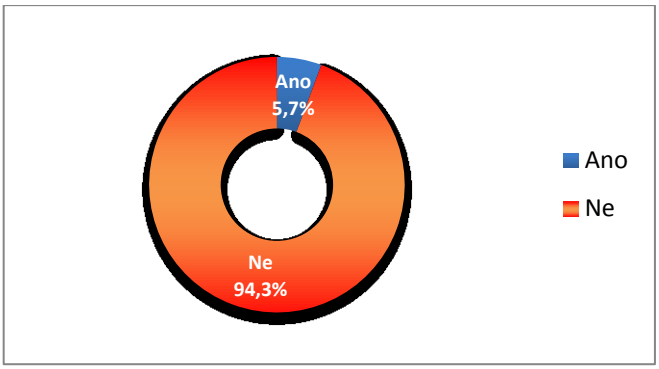
S problémem spamu v komunikaci se v současné informační době potýká mnoho uživatelů. Vzhledem k odpovědím lze konstatovat, že tuto problematiku má útvar CIT dostatečně zabezpečenou a spam úspěšně filtruje. Více jak polovina uživatelů se vůbec nepotýká s nevyžádanou poštou. V případě nějakého výskytu spamu, se takto děje ojediněle.



Graf 3.16 Jak často se setkáváte s problémem nevyžádané pošty (tzv. Spam) na Vašem univerzitním e-mailu?; vlastní zpracování

Otázka č. 15 - Během práce v rámci univerzity, setkali jste se s nějakým bezpečnostním incidentem?

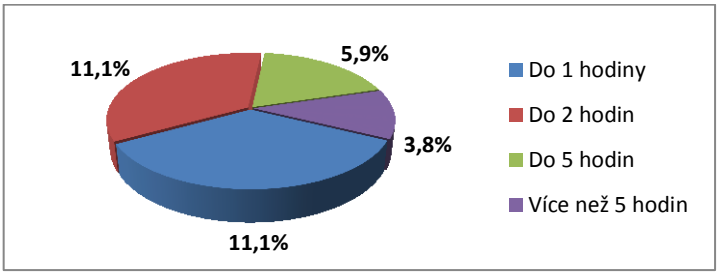
Otázka bezpečnostních incidentů v současnosti s rozvojem informačních technologií neustále roste a je potřeba této problematice věnovat velkou pozornost. Příjemným zjištěním dle získaných výsledků je, že 94% respondentů se během svého působení na univerzitě nesetkalo s nějakým bezpečnostním incidentem. Zbylých téměř 6% uživatelů nějaký incident zaznamenalo, což pravděpodobně souvisí s předchozí otázkou týkající se spamu.



Graf 3.17 Během práce v rámci univerzity, setkali jste se s nějakým bezpečnostním incidentem?; vlastní zpracování

Otázka č. 16 - Jak brzy zareagovali pracovníci útvaru CIT při řešení bezpečnostního incidentu?

Tato otázka nebyla povinná a byla úzce spojena s předchozí otázkou, tedy po jak dlouhé době oddělení CIT zareagovalo na podnět o výskytu bezpečnostního incidentu. Odpovídat především měli ti respondenti, kteří se setkali s nějakým bezpečnostním incidentem. Ovšem součet odpovědí neodpovídá počtu odpovědí (odpovědi typu Ano) z předchozí otázky a data tak nelze považovat za relevantní.

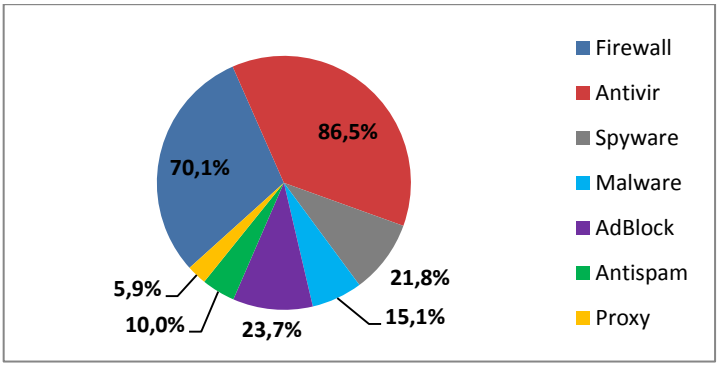


Graf 3.18 Jak brzy zareagovali pracovníci útvaru CIT při řešení bezpečnostního incidentu?; vlastní zpracování

Otázka č. 17 - Jaké využíváte bezpečnostní nástroje v rámci zabezpečení Vašeho osobního počítače, ze kterého přenášíte data na univerzitní PC?

Otázka se zaměřuje na softwarové prostředky pro zajištění bezpečnosti. Běžně uživatelé kombinují více takových nástrojů, proto studenti opět mohli vybrat více odpovědí. Během práce v rámci univerzitní sítě je zapotřebí, aby uživatelé byli rovněž vybaveni potřebnými nástroji pro zajištění bezpečnosti proti potenciálním hrozbám. Ovšem takové nástroje se dnes spíše považují za základní vybavení počítače uživatele. Výsledky dopadly podle očekávání, v převážné většině uživatelé využívají antivir (87%) a firewall (70%). Poté jsou tyto nástroje

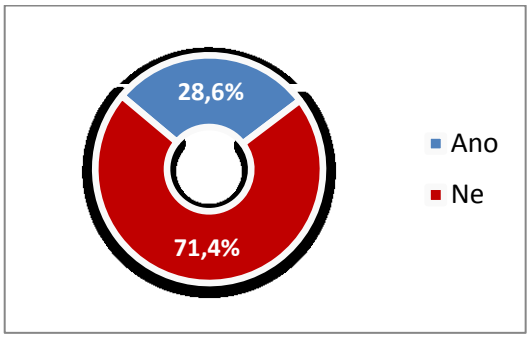
různě doplňovány o nástroje na detekci a odstranění Spyware a nástroje AdBlock, zabraňující zobrazování a vyskakování nežádoucích reklam na internetu.



Graf 3.19 Jaké využíváte bezpečnostní nástroje v rámci zabezpečení Vašeho osobního počítače, ze kterého přenášíte data na univerzitní PC?; vlastní zpracování

Otázka č. 18 - Sledujete trendy v oblasti informační bezpečnosti?

Pravidelná informovanost o nových bezpečnostních opatřeních a jejich včasná implementace funguje jako prevence proti nežádoucím jevům v podobě útoků apod. Poněkud překvapivým výsledkem dopadlo šetření, zda studenti věnují pozornost současným trendům informační bezpečnosti. V zaznamenaných 71% případů si studenti nedoplňují informace o nových možnostech v oblasti zabezpečení informací a komunikace, což může sehrát určitou roli v ohledu aplikace bezpečnostních opatření.

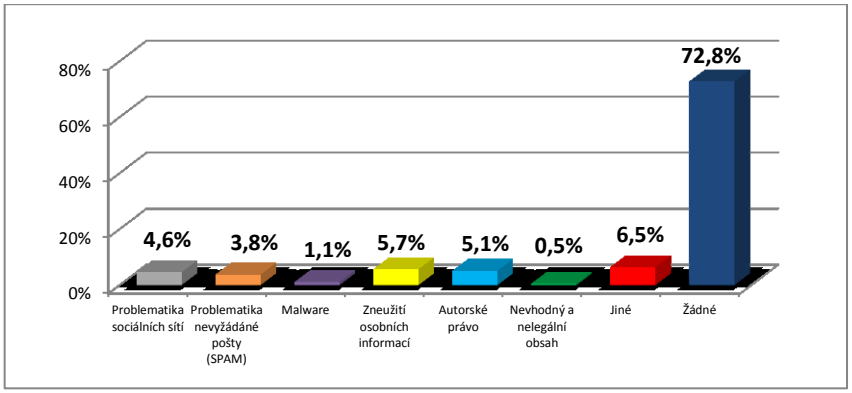


Graf 3.20 Sledujete trendy v oblasti informační bezpečnosti?; vlastní zpracování

Otázka č. 19 - Zúčastnili jste se někdy přednášky či kurzu zaměřených na problematiku informační bezpečnosti?

Stejně jako u předchozí otázky, i zde se sleduje zájem o informace v podobě absolvování nějaké přednášky, kurzu či diskuse na téma informační bezpečnosti. I co se týče výsledku odpovědí, který je s předchozí otázkou podobný, jednoznačně vypovídá o tom, že studenti neprojevují příliš velký zájem o informace z oblasti informační bezpečnosti. Z ostatních

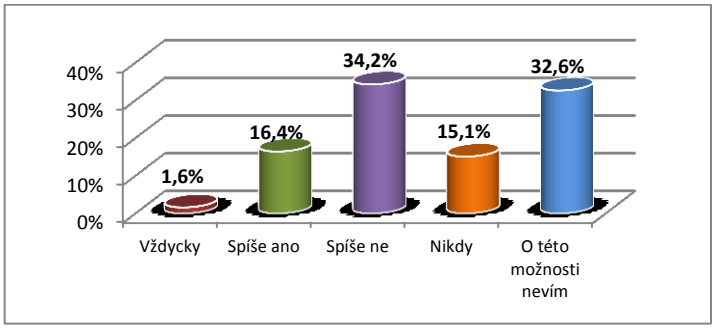
odpovědí lze předpokládat, že se jedná o studenty, jejichž studium se věnuje informačním technologiím.



Graf 3.21 Zúčastnili jste se někdy přednášky či kurzu zaměřený na problematiku informační bezpečnosti?; vlastní zpracování

Otázka č. 20 - Využíváte v rámci vyhledávání informací na internetu funkci tzv. Anonymního prohlížení?

Současné webové prohlížeče nabízí řadu funkcí a nástrojů, které jsou implementovány vývojáři těchto typů softwaru. Jednou z takových funkcionalit je možnost anonymního prohlížení, kdy si prohlížeč neuchovává žádná data (osobní údaje, hesla atd.) během celého sezení uživatele. Díky tomu prohlížeč funguje jako prevence proti zneužití osobních údajů. Celá jedna třetina ze všech respondentů o takové funkcionalitě nemá tušení. Dá se říci, že 16% studentů většinou využívá funkci anonymního prohlížení. Zbylé odpovědi napovídají, že uživatelé o této možnosti vědí, ale nevyužívá ji.

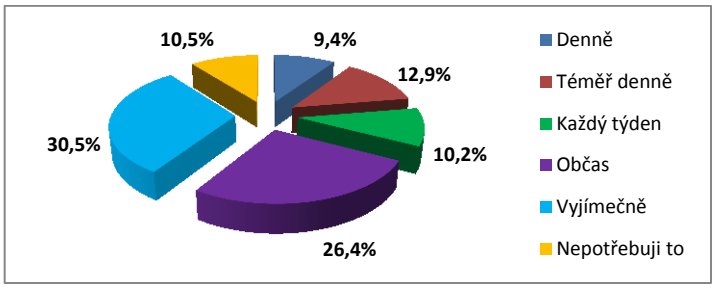


Graf 3.22 Využíváte v rámci vyhledávání informací na internetu funkci tzv. Anonymního prohlížení?; vlastní zpracování

Otázka č. 21 - Jak často stahujete nějaký obsah z internetu v rámci připojení v univerzitní síti?

Stahování různého obsahu může mnohdy vyvolat nežádoucí jevy a je zapotřebí těmto aktivitám věnovat zvýšenou pozornost. Stahované data mohou obsahovat škodlivý kód, který

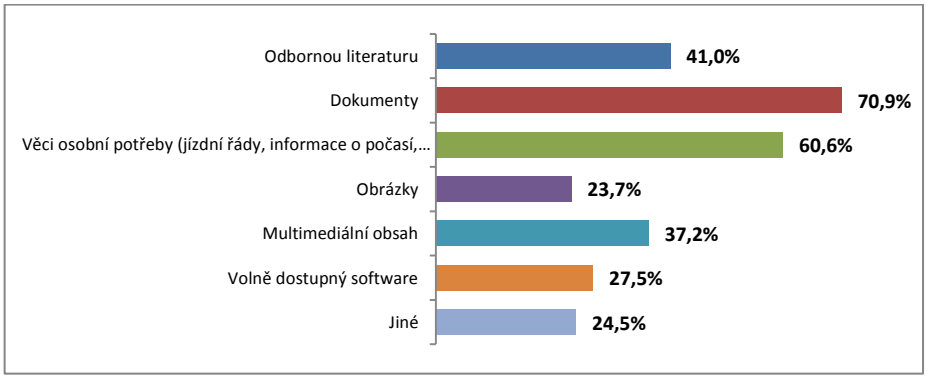
prostupuje do vnitra počítače a mohou tak narušit jeho chod. Z následujících výsledků lze konstatovat, že nadpoloviční většina uživatelů stahují obsah občas či pouze výjimečně. Někteří vůbec data nestahují. Důvodem může být současná dostupnost libovolného obsahu bez nutnosti jeho stahování do počítače. U dalších otázek jsou odpovědi respondentů poměrně shodně rozděleny. Celkově 23% dotázaných stahuje nějaký obsah denně či téměř denně.



Graf 3.23 Jak často stahujete nějaký obsah z internetu v rámci připojení v univerzitní síti?; vlastní zpracování

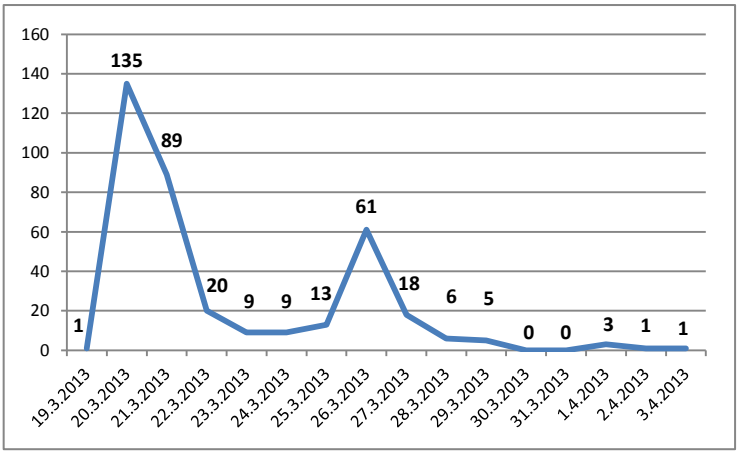
Otázka č. 22 - Jaký obsah nejčastěji stahujete?

V otázce informační bezpečnosti je nutné věnovat pozornost konkrétnímu typu stahovaného obsahu. Dnes už neplatí, že škodlivý kód sebou mohou nést pouze spustitelné programy či multimediální soubory. Následující otázka vypovídá o charakteru nejčastěji stahovaného obsahu uživateli. Rovněž i zde mohli studenti volit více odpovědí, protože většinou se uživatelé nesoustředí pouze na jeden typ obsahu. Z výsledků vyplývá, že nejčastěji stahovaným obsahem jsou dokumenty (71%) a informace pro osobní potřebu (61%). Dále uživatelé nejvíce stahují odbornou literaturou nebo soubory multimediálního typu v podobě audio a video záznamů apod.



Graf 3.24 Jaký obsah nejčastěji stahujete?; vlastní zpracování

Následující graf zachycuje počty respondentů v jednotlivých dnech. Absolutní špička nastala v době prvního nasazení prostřednictvím sociálních skupin, kdy v tento den odpovědělo 135 studentů, poté tento trend klesal. Další nárůst byl zaznamenán 26. 3. 2013, kdy odpovědělo 61 respondentů, jakožto výsledek způsobený opětovným připomenutím a zveřejněním dotazníku mezi potenciální respondenty.



Graf 3.25 Vývoj odpovědí v jednotlivých dnech; vlastní zpracování

4 Vyhodnocení analýzy a návrh opatření ke zvýšení bezpečnosti IS

4.1 Použité metodiky analýzy

Z hlediska struktury dotazníku a získaných dat byly v rámci analýzy dosažených výsledků použity dvě statistické metody, jimiž jsou regresní analýza, korelační analýza a párový t-test. V rámci veškerých analýz prováděných nad získanými daty byly použity softwarové nástroje Excel ze sady Microsoft Office a statistický PASW Statistics 18.

4.1.1 Regresní analýza

Regresní analýza se používá při zkoumání závislostí dvou a více číselných proměnných. Je to souhrn statistických metod a postupů, sloužících k odhadu hodnot nebo středních hodnot nějaké proměnné, odpovídající daným hodnotám jedné či většího počtu vysvětlujících proměnných. Snahou regresní analýzy je nalézt idealizující matematickou funkci takovou, aby co nejlépe vyjadřovala charakter závislosti a co nejvěrněji zobrazovala průběh změn podmíněných průměrů závisle proměnné. Tato svojí podstatou hypotetická funkce se nazývá regresní funkce. Cílem regresní analýzy je co nejlepší přiblížení empirické (vypočítané) regresní funkce k hypotetické regresní funkci. Podkladem pro regresní analýzu jsou vždy nějaká data získaná pozorování (zjišťováním). O těchto údajích předpokládáme, že byly získány náhodným výběrem. Důležitou otázkou, kterou je třeba při volbě regresní funkce posuzovat, je korelovanost regresorů figurujících v regresní funkci. Silně korelované regresory by v regresní funkci neměly být. Výběrová regresní funkce:[67]

$$Y = \beta_0 x_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_m x_m$$

kde $\beta_0, \beta_1, \beta_2, .., \beta_m$ jsou bodové odhady parametrů regresní funkce a $x_0, x_1, x_2, ..., x_m$ jsou známé funkce jedné či několika vysvětlujících proměnných, které se někdy nazývají regresory. Často jsou vhodnými bodovými odhady regresních parametrů odhady pořízené metodou nejmenších čtverců.[68]

[67] OPLUŠTILOVÁ, Irena a Michaela TULISOVÁ. Elementární statistické metody a jejich věcný význam: Regresní a korelační analýza. [online]. 2003 [cit. 2013-04-17]. Dostupné z: http://www.regionalka.wz.cz/reg%20info/Elementarni%20%20stat.%20metody.htm
[68] Tamtéž.

4.1.2 Korelační analýza

Posuzuje vzájemné vztahy pomocí různých měr závislosti, většinou pomocí různých korelačních koeficientů. Nejpoužívanější mírou těsnosti vztahu dvou spojitých znaků je Pearsonův korelační koeficient. Je mírou linearity vztahu (jak těsně se body přimykají k přímce). Pearsonův korelační koeficient se značí r a pro hodnoty r platí: $-1 \leq r \leq 1$. Hodnoty ± 1 nabývá tehdy, když veličiny jsou absolutně závislé, tzn., pokud sestrojíme bodový graf dvojice zkoumaných veličin, všechny body leží na přímce. Pokud $r = 0$ (nebo nabývá hodnoty blízké nule), veličiny jsou nezávislé. Kladné hodnoty korelačního koeficientu znamenají pozitivní závislost, obě veličiny zároveň rostou nebo klesají. Záporné hodnoty korelačního koeficientu znamenají negativní závislost, jedna veličina roste, zatímco druhá klesá. Míru závislosti podle absolutní hodnoty Pearsonova korelačního koeficientu obvykle interpretujeme:[69]

- 0,1 – 0,3 korelace slabá,
- 0,4 – 0,6 korelace střední,
- 0,7 – 0,8 korelace silná,
- nad 0,9 korelace velmi silná.

4.1.3 Dvouvýběrový párový t-test na střední hodnotu

Párový test se používá v případě, že jsou pozorování ve výběrech přirozeným způsobem spárována, například při dvojím testování skupiny - před experimentem a po něm. Tento analytický nástroj provede pomocí příslušných vzorců párový Studentův t-test pro dva výběry, který určí, zda je pravděpodobné, že pozorování před provedením akce a pozorování po provedení akce pocházejí z rozdělení se stejnými středními hodnotami souborů. Při tomto typu t-testu se nepředpokládá, že se rozptyly obou souborů rovnají. Jedním z výsledků, které tento nástroj vypočítává, je společný rozptyl, tj. akumulovaná míra rozptýlení dat od střední hodnoty.[70]

[69] *III. cvičení ze statistiky* [online]. Olomouc [cit. 2013-04-17]. Dostupné z: http://ulb.upol.cz/praktikum/statistika3.pdf. UPOL.

[70] Nástroje statistické analýzy. *Microsoft Corporation* [online]. [cit. 2013-04-17]. Dostupné z: http://office.microsoft.com/cs-cz/excel-help/nastroje-statisticke-analyzy-HP005203873.aspx

4.2 Analýza získaných dat

Za pomocí softwarových nástrojů Microsoft Office Excel a PASW Statistics 18 byly prováděny analýzy, pomocí kterých se hledaly jednotlivé závislosti mezi získanými daty z dotazníku. Následující přehled obsahuje rozbor vybraných závislostí. Jednotlivé výsledky vychází ze stupnice významnosti definované v kapitole 4.2.2. V rámci zpracování výsledků je zapotřebí pamatovat na přítomnost chyb, které mohou pramenit z vyplňování dotazníků prostřednictvím internetu, a nelze tak předpokládat jednoznačné výsledky. Pro přesnější výsledky by museli jednotliví respondenti odpovídat během osobního kontaktu s tazatelem.

Popis situace: **1 - Analýza vztahu preferencí uživatelů a jimi využívaných prohlížečů**
U otázky týkající se používaných webových prohlížečů měli studenti možnost vybrat i více prohlížečů, které preferují pro procházení internetových stránek. Protože uživatelé nepoužívají pouze jeden prohlížeč, ale ve většině případů jich používají více z důvodu potenciální problému s otevřením webového obsahu. Cílem bylo zjistit, jestli mezi užívanými prohlížeči existuje náklonost uživatelů k využívání daných prohlížečů.

Stanovení hypotéz

H_0: Existuje vztah mezi uživatelskými preferencemi jimi využívaných prohlížečů

H_1: Neexistuje vztah mezi uživatelskými preferencemi jimi využívaných prohlížečů

Correlations

		Google Chrome	Mozilla Firefox
Google Chrome	Pearson Correlation	1	-,433**
	Sig. (2-tailed)		,000
	N	371	371
Mozilla Firefox	Pearson Correlation	-,433**	1
	Sig. (2-tailed)	,000	
	N	371	371

**. Correlation is significant at the 0.01 level (2-tailed).

Tab. 4.1 Korelační matice testovaných prohlížečů; vlastní zpracování

Závěr hypotézy

Na základě zjištěných hodnot Pearsonova korelačního koeficientu, sledující závislosti mezi používanými prohlížeči, byla zjištěna středně velká závislost (r = 0,433) dle rozdělení významnosti mezi prohlížeči Google Chrome a Mozilla Firefox. Z toho vyplývá, že uživatelé, kteří si na své zařízení nainstalují Google Chrome, si rovněž nainstalují i Mozillu Firefox. Proto přijímáme hypotézu H_0.

Popis situace: **2 - Analýza vztahu mezi uživateli sledující trendy informační bezpečnosti**
Další zkoumanou oblastí je zjištění vazeb mezi vnímáním uživatelů. Tedy zda uživatelé, kteří sledují trendy v problematice informační bezpečnosti, se účastní nějakých přednášek či diskusí zaměřených právě na oblast informační bezpečnosti a zda využívají bezpečnostních funkcí v rámci svých preferovaných prohlížečů. U takových uživatelů se předpokládá kladný vztah k informační bezpečnosti.

Stanovení hypotéz

H_0: Existuje vztah mezi zájmem uživatelů o bezpečnost informací a jejich zvyklostmi
H_1: Neexistuje vztah mezi zájmem uživatelů o bezpečnost informací a jejich zvyklostmi

Correlations

		fakulta	trendy v bezepčnosti	přednáška o bezpečnosti	anonymní funkce
Pearson Correlation	fakulta	1,000	-,149	,012	-,053
	trendy v bezepčnosti	-,149	1,000	,323	,287
	přednáška o bezpečnosti	,012	,323	1,000	,236
	anonymní funkce	-,053	,287	,236	1,000
Sig. (1-tailed)	fakulta	.	,002	,406	,152
	trendy v bezepčnosti	,002	.	,000	,000
	přednáška o bezpečnosti	,406	,000	.	,000
	anonymní funkce	,152	,000	,000	.
N	fakulta	371	371	371	371
	trendy v bezepčnosti	371	371	371	371
	přednáška o bezpečnosti	371	371	371	371
	anonymní funkce	371	371	371	371

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,164[a]	,027	,019	1,688	1,921

a. Predictors: (Constant), anonymní funkce, přednáška o bezpečnosti, trendy v bezepčnosti

b. Dependent Variable: fakulta

Tab. 4.2 Korelační matice a regresní model uživatelů sledujících trendy informační bezpečnosti; vlastní zpracování

Závěr hypotézy

Na základě zjištěných významných hodnot korelačních koeficientů (r_1 = 0,323, r_2 = 0,287), lze potvrdit, že existuje slabá závislost mezi sledovanými proměnnými. Uživatelé, sledující současné trendy v oblasti informační bezpečnosti, aplikují nabyté znalosti do svého počínání v informačním světě a jeho praktik zabezpečení. A rovněž rozšiřují své znalosti prostřednictvím přednášek týkající se informační bezpečnosti. Proto můžeme přijmout hypotézu H_0. Avšak bylo by vhodné provést další průzkum, který by potvrdil nebo vyvrátil tuto slabou závislost.

Popis situace: **3 - Analýza rozdílnosti využívání bezdrátových sítí dle fakult**

Studenti během svého studia mohou neustále využívat bezdrátové připojení. V rámci jeho využití různými obory a fakultami by mohl být rozdíl, protože existují obory, které jej v rámci svého zaměření příliš nepotřebují. Pak jsou obory, např. Fakulta elektrotechniky a informatiky, jejichž obory si přímo vyžadují využívání bezdrátových sítí a může tam existovat větší využitelnost oproti ne tolik technickým oborům.

Stanovení hypotéz

H_0: Možnost bezdrátového připojení je zásadnější pro technické obory

H_1: Možnost bezdrátového připojení není zásadní pouze pro technické obory

Correlations

		důležitost wifi	fakulta
Pearson Correlation	důležitost wifi	1,000	-,124
	fakulta	-,124	1,000
Sig. (1-tailed)	důležitost wifi	.	,008
	fakulta	,008	.
N	důležitost wifi	371	371
	fakulta	371	371

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,124[a]	,015	,013	1,093	1,972

a. Predictors: (Constant), fakulta

b. Dependent Variable: důležitost wifi

Tab. 4.3 Korelační matice a regresní model důležitosti bezdrátového připojení v závislosti na fakultách; vlastní zpracování

Závěr hypotézy

V tomto případě jsou hodnoty korelačních koeficientů i koeficientu determinace velice nízké ($R = 0{,}124$ a $r = 0{,}124$), tudíž lze konstatovat, že využívání bezdrátových sítí je stejně důležité pro obory různého zaměření, tedy jak technické, tak i netechnické obory. Proto můžeme zamítnout hypotézu H_0 a přijmout alternativní hypotézu H_1.

Popis situace: **4 - Analýza vztahu ve volbě hesel**

Nyní bylo předmětem analýzy zkoumat, zda existují vazby ve výběru vhodných hesel uživateli. Vhodným heslem se předpokládá heslo s délkou minimálně 8 znaků a kombinování různých znaků různé velikosti. Taková hesla se považují za bezpečná a nesnadně

dekódovatelné. Předpokládá se, že uživatelé s výběrem dlouhých (silných) hesel budou rovněž užívat vhodné kombinace znaků svých hesel.

Stanovení hypotéz

H_0: Existuje vztah uživatelů k volbě kombinace znaků hesla a zároveň dlouhým (silným) heslům

H_1: Neexistuje vztah uživatelů k volbě kombinace znaků hesla a zároveň dlouhým (silným) heslům

Correlations

		typy hesla	délka hesla	změna hesla - perioda
Pearson Correlation	typy hesla	1,000	,273	-,191
	délka hesla	,273	1,000	-,080
	změna hesla - perioda	-,191	-,080	1,000
Sig. (1-tailed)	typy hesla	.	,000	,000
	délka hesla	,000	.	,063
	změna hesla - perioda	,000	,063	.
N	typy hesla	371	371	371
	délka hesla	371	371	371
	změna hesla - perioda	371	371	371

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,321[a]	,103	,098	,875	1,986

a. Predictors: (Constant), změna hesla - perioda, délka hesla

b. Dependent Variable: typy hesla

Tab. 4.4 Korelační matice a regresní model vztahu ve volbě hesel; vlastní zpracování

Závěr hypotézy

Výsledné hodnoty koeficientů (r = 0,273 a R = 0,321) vyjadřují slabou závislost dle rozdělení významnosti, avšak nelze potvrdit vztah mezi sledovanými proměnnými. Uživatelé používají dlouhá hesla a zároveň volí kombinovaná hesla. Z tohoto důvodu můžeme přijmout hypotézu H_0, ale bylo by tady zapotřebí provést další průzkum pro potvrzení nebo vyvrácení slabé závislosti.

Popis situace: **5 - Analýza vztahu mezi informovanými uživateli a počtem aplikovaných bezpečnostních opatření na jejich zařízeních**

Další zkoumanou oblastí je zjištění závislosti mezi uživateli, kteří sledují moderní trendy informační bezpečnosti a počtem jimi užívaných bezpečnostních opatření. Dá se předpokládat, že uživatel, který se zajímá o problematiku informační bezpečnosti, tak díky svým nabytým znalostem bude využívat větší množství bezpečnostních opatření a nástrojů.

Stanovení hypotéz

H_0: Existuje vztah mezi uživatelem sledujícím trendy a počtem jimi využívaných bezpečnostních nástrojů

H_1: Neexistuje vztah mezi uživatelem sledujícím trendy a počtem jimi využívaných bezpečnostních nástrojů

Correlations

		trendy v bezepčnosti	SUMbeznastr
Pearson Correlation	trendy v bezepčnosti	1,000	-,293
	SUMbeznastr	-,293	1,000
Sig. (1-tailed)	trendy v bezepčnosti	.	,000
	SUMbeznastr	,000	.
N	trendy v bezepčnosti	371	371
	SUMbeznastr	371	371

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,293[a]	,086	,083	,433	1,826

a. Predictors: (Constant), SUMbeznastr

b. Dependent Variable: trendy v bezepčnosti

Tab. 4.5 Korelační matice a regresní model vztahu mezi informovaností a počtem nástrojů; vlastní zpracování

Závěr hypotézy

Zjištěné hodnoty korelačních koeficientů a koeficientu determinace (r = 0,293 a R = 0,293) vyjadřují slabou závislost mezi zájmem uživatelů o informační bezpečnost a počtem nástrojů, které využívají pro zabezpečení svých zařízení před hrozbami. Proto můžeme přijmout hypotézu H_0. Opět i v tomto případě by bylo vhodné provést další průzkum pro přesnější rozhodnutí závislosti.

Popis situace: **6 - Sledování vztahu mezi důležitostí bezdrátového připojení a počtem zařízení každého uživatele připojovaných do univerzitní sítě**

Cílem tohoto testu bylo hledání závislosti mezi použitými zařízeními pro připojení do bezdrátové sítě a důležitostí bezdrátového připojení na univerzitě. V rámci testování museli být upraveny data s používanými zařízeními a to tak, že se použil pouze vybraný soubor dat obsahující počet používaných zařízení, korespondujících s každým respondentem. Konkrétně se sleduje, zda určitý počet zařízení daného uživatele vysvětluje důležitost bezdrátového připojení.

Stanovení hypotéz

H_0: Existuje závislost mezi počtem připojovaných zařízení a důležitostí bezdrátového připojení

H_1: Neexistuje závislost mezi počtem připojovaných zařízení a důležitostí bezdrátového připojení

Correlations

		SUM	důležitost wifi
Pearson Correlation	SUM	1,000	-,336
	důležitost wifi	-,336	1,000
Sig. (1-tailed)	SUM	.	,000
	důležitost wifi	,000	.
N	SUM	371	371
	důležitost wifi	371	371

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,336[a]	,113	,111	,638	2,135

a. Predictors: (Constant), důležitost wifi

b. Dependent Variable: SUM

Tab. 4.6 Korelační matice a regresní model vztahu mezi důležitostí Wi-Fi a počtem zařízení; vlastní zpracování

Závěr hypotézy

Podle zjištěných hodnot korelačního a determinačního koeficient (r = R = 0,336) nebyl zjištěn výrazný vztah mezi těmito dvěma proměnnými, avšak slabší závislost se zde vyskytuje. Na základě dosažených výsledků lze potvrdit, že čím více zařízení daný student využívá k připojení do univerzitní bezdrátové sítě, tím je pro něj toto připojení zásadnější. Proto můžeme přijmout hypotézu H_0. Opět by bylo vhodné provést další průzkum pro jednoznačné určení hypotézy a závislosti mezi těmito proměnnými.

Popis situace: **7 - Sledování zájmu studentů ekonomické fakulty o informační bezpečnost**

Během tohoto testování byly použity pouze data od respondentů ekonomické fakulty. Předmětem analýzy bylo zjistit zájem studentů této fakulty o informační bezpečnost. Konkrétně šlo o hledání závislostí mezi sledováním současných trendů, navštěvování přednášek týkajících se informační bezpečnosti a aplikací znalostí v podobě využívání anonymního prohlížení stránek.

Stanovení hypotéz

H_0: Existuje vztah mezi sledováním, navštěvováním a využíváním znalostí v rámci bezpečnosti informací u studentů ekonomické fakulty

H_1: Neexistuje vztah mezi sledováním, navštěvováním a využíváním znalostí v rámci bezpečnosti informací u studentů ekonomické fakulty

Correlations

		trendy v bezepčnosti	přednáška o bezpečnosti	anonymní funkce
Pearson Correlation	trendy v bezepčnosti	1,000	,367	,477
	přednáška o bezpečnosti	,367	1,000	,361
	anonymní funkce	,477	,361	1,000
Sig. (1-tailed)	trendy v bezepčnosti	.	,000	,000
	přednáška o bezpečnosti	,000	.	,000
	anonymní funkce	,000	,000	.
N	trendy v bezepčnosti	85	85	85
	přednáška o bezpečnosti	85	85	85
	anonymní funkce	85	85	85

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	,521[a]	,272	,254	,405	2,040

a. Predictors: (Constant), anonymní funkce, přednáška o bezpečnosti

b. Dependent Variable: trendy v bezepčnosti

Tab. 4.7 Korelační matice a regresní model studentů ekonomické fakulty ve vztahu k informační bezpečnosti; vlastní zpracování

Závěr hypotézy

Na základě získaných výsledků (r_1 = 0,367, r_2 = 0,477 a R = 0,521) bylo dosaženo překvapivých výsledků, což může být způsobeno velkým počtem respondentů informatického zaměření. Avšak konkrétní číslo těchto respondentů nelze z odpovědí zjistit. Podle hodnot koeficientů mezi těmito proměnnými existuje slabý až středně velký statistický vztah. Tento vztah vyjadřuje zájem studentů o problematiku informační bezpečnosti, kdy každý kdo se zajímá o nejnovější trendy bezpečnosti informací, tak se účastní i přednášek zaměřených na toto téma. Zároveň využívají nabytých znalostí formou jako je např. funkce anonymního prohlížení. Proto můžeme přijmout hypotézu H_0.

4.3 Shrnutí výsledků dvouvýběrových párových t-testů

V rámci analýzy byly vybrané oblasti rovněž zpracovány pomocí párových t-testů, ve kterých se porovnávala data mezi studenty fakulty elektrotechniky a informatiky (FEI) a studenty ostatních fakult. Lze předpokládat, že studenti elektrotechniky a informatiky budou mít k problematice informační bezpečnosti blíže než studenti zbylých fakult. V testu byla porovnávána data stejných oblastí. V případě nejasných výsledků byly tyto testy ověřeny pomocí testu ANOVA. Veškeré testy byly prováděny na hladině významnosti 5%.

Konkrétně při srovnávání v oblasti volby kombinací hesla by se dalo předpokládat, že studenti IT budou volit složitější hesla. Po t-testu se ukázala mírná rozdílnost, avšak po provedení analýzy rozptylu (ANOVA) se tento rozdíl nepotvrdil. Z toho vyplývá, že studenti volí svá hesla stejným způsobem bez rozdílu příslušnosti dané fakulty. V dalším případě na základě srovnání důležitosti bezdrátového připojení bylo zjištěno, že studenti FEI považují bezdrátové připojení jako součást univerzity za důležitější než ostatní studenti. Stejně tak se projevil rozdíl v počtu využívaných zařízení pro připojení do bezdrátové sítě, kdy opět studenti FEI používají o něco více zařízení než studenti ostatních fakult. Podle předpokladů se naplnilo i očekávání, že studenti FEI se zajímají o informační bezpečnost ve větší míře, než je tomu u studentů ostatních fakult.

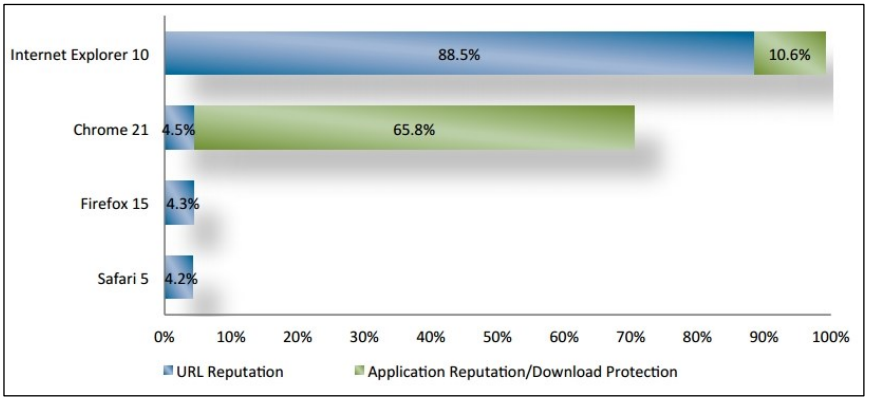
Zajímavým výsledkem však je zjištění, že studenti ostatních fakult si mění hesla pro přístup do univerzitního systému častěji než studenti FEI, avšak nelze potvrdit vztah mezi těmito soubory. V ostatních sledovaných případech se tyto dvě skupiny studentů nějak zásadně neliší. Všechny provedené párové t-testy, které potvrzují výše uvedené výsledky, jsou uvedeny v Příloze 8.

4.4 Studie internetových prohlížečů

Každoročně probíhá srovnávání na základě testování internetových prohlížečů dle různých kritérií. Jedním z těchto kritérií je mimo jiné i testování bezpečnosti prohlížečů, tedy jak si dokáží poradit s útočníky a blokováním internetových útoků a webových stránek, které jsou napadeny škodlivým kódem či phisingem. Tuto studii provádí nezávislá organizace NSS Labs. Předmětem testování jsou prohlížeče Mozilla Firefox, Google Chrome, Internet Explorer a Safari. V některých testech figuruje i prohlížeč Opera. Poslední test této organizace pochází z října roku 2012 a je znázorněn na obrázku Obr. 4.1.

Útoky sociálního inženýrství, které se snaží lidi přes internet podvést za účelem získání jejich citlivých dat nebo utajených informací jejich firmy, patří mezi největší internetové hrozby současnosti. Výběr prohlížeče může sehrát klíčovou roli v tom, zda zůstaneme v online světě v bezpečí nebo ne.[71]

[71] Internet Explorer blokuje podle NSS Labs sedmkrát více útoků než konkurence. *ICT Security* [online]. 2011 [cit. 2013-04-17]. Dostupné z: http://www.ictsecurity.cz/sk/security-bezpenos/internet-explorer-blokuje-podle-nss-labs-sedmkrat-vice-utok-ne-konkurence.html



Obr. 4.1 Srovnání internetových prohlížečů

Zdroj: NSS LABS. Browser Security Comparative Analysis: Socially Engineered Malware [online], 2012, www.nsslabs.com

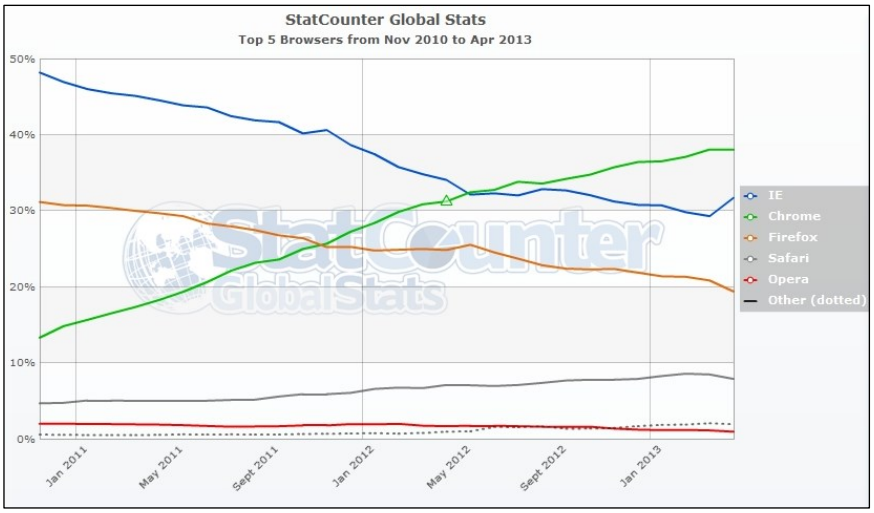
Podle aktuální studie NSS Labs je Internet Explorer 10 stále nejbezpečnějším prohlížečem. Internet Explorer 10 dokázal v testu NSS Labs zablokovat 88,5% všech útoků, se zapnutou filtrovací funkcí tzv. SmartScreen Application Reputation byl tento podíl dokonce 99,1 %. Druhým v pořadí úspěšnosti je prohlížeč Google Chrome 21, který dokázal zastavit pouze 4,5% všech nebezpečných útoků snažících se zaútočit škodlivým kódem na uživatelskou stanici. Avšak za pomoci prostředí sandbox Application Reputation bylo u tohoto prohlížeče odraženo celých 70,3% útoků. U prohlížečů Mozilla Firefox 15 a Safari 5 to bylo pouze 4,3% a 4,2% zablokovaných útoků a v tomto testu naprosto propadly. Poslední dva zmíněné prohlížeče neobsahují funkci typu Application Reputation.[72]

Funkce SmartScreen URL Reputation s využitím celosvětové databáze kontroluje stránky na přítomnost škodlivých kódů. Díky ní je prohlížeč, podporující tuto funkci, schopen zablokovat větší procento možných útoků. Funkce SmartScreen Application Reputation stejným způsobem provádí kontrolu stahovaných souborů.[73]

Následující obrázek Obr. 4.2 znázorňuje vývoj pěti nejoblíbenějších webových prohlížečů v období od listopadu 2010 do dubna roku 2013. Z jednotlivých trendů si lze všimnou, že největší nárůst preferencí uživatelů zaznamenal Google Chrome. Tento fakt jen potvrzuje výsledek dotazníkového šetření v rámci diplomové práce, který byl zaznamenán u otázky týkající se nejpoužívanějších prohlížečů z řad studentů. Konkurenční prohlížeče Mozila Firefox a Intenet Explorer s časem klesají v oblíbenosti ze strany uživatelů, přičemž největší

[72] Číselné údaje čerpány z NSS Labs.
[73] ICT SECURITY, ref. 71.

pokles se projevil právě u nejrozšířenějšího prohlížeče Internet Explorer. Avšak v posledních měsících zaznamenal menší nárůst a bylo by zajímavé sledovat, zda tento trend bude mít stejný průběh. Naopak nejméně užívaným prohlížečem je Opera. I přes upadající oblíbenost u uživatelů se prohlížeč Internet Explorer stále řadí mezi nejvíce užívanými na světě.



Obr. 4.2 Vývoj oblíbenosti současných prohlížečů
Zdroj: STATCOUNTER. Top 5 Browsers from Nov 2010 to Apr 2013 [online], gs.statcounter.com

V poslední době se častým cílem útoků stávají také zásuvné moduly (tzv. plug-iny) prohlížečů, které jsou v dnešní době oblíbené a uživatelům nabízí možnost rozšíření svých prohlížečů o zajímavé aplikace a nástroje. V rámci bezpečnostních opatření, integrovaných u jednotlivých prohlížečů, hraje důležitou roli také intenzita zveřejňování nových opravných aktualizací prohlížečů ze strany jejich tvůrců. Stejně jako např. antivirové programy jsou účinné pouze v případě, kdy je neustále aktualizována jejich virová databáze, tak i webové prohlížeče potřebují pravidelné aktualizace, které přináší různé druhy oprav, záplat, integraci nových prostředků apod. Výhodou u dnešních webových prohlížečů je vlastnost, že uživatel nemusí sledovat vydávání pravidelných aktualizaci, ale prohlížeče sami kontrolují dostupnost nejnovějších aktualizací.

4.5 Současný stav zajištění bezpečnosti ICT

Tento proces v rámci metodiky COBIT, DS5 Zajištění bezpečnosti systémů, je samostatně vyhodnocen, protože představuje velmi důležitý segment řízení ICT. Na úrovni CIT je

informační bezpečnost chápána spíše technicky, jako zabezpečení sítě a aplikací. V rámci tohoto pohledu je bezpečnost na kvalitní úrovni a lze konstatovat, že:[74]

- je vytvořen funkční tým pro řešení bezpečnostních incidentů na síti - CSIRT;
- ve směrnicích, jejichž garantem je CIT, je bezpečnosti informací věnován důraz;
- je velmi dobře zpracován systém pro autentizaci a autorizaci uživatelů;
- proces přidělování oprávnění je částečně formalizován (včetně odebírání oprávnění);
- není dedikován pracovník na pozici bezpečnostního manažera;
- bezpečnost informací je v organizaci vnímána slabě;
- není prováděno školení pracovníků v rámci zvyšování bezpečnostního povědomí.

Ochrana informací je na úrovni 1 v rámci modelu procesní vyspělosti (CMM). Tomu odpovídá neexistence řízení bezpečnosti informací a řešení jednotlivých oblastí ad hoc. Opět chybí formální zpětné vazby a vyhodnocování dosažených cílů. Především však není zaveden komplexní pohled na bezpečnost informací v celé šíři této problematiky. Jako strategický cíl se doporučuje zavedení ISMS na úrovni řízení CIT. Toto by mělo být v souladu s ISO/IEC 27001, jeho zavedení však v současné době není indikováno jako nezbytně nutné. Toto doporučení je zároveň v souladu s procesem PO9 - Hodnocení a řízení rizik a DS5 - Zajištění bezpečnosti systémů dle COBITu.[75]

4.6 Návrh opatření pro zajištění informační bezpečnosti

Na základě zjištěných výstupů lze posoudit, které oblasti jsou v rámci informační bezpečnosti a celkového IT univerzity klíčové. Proto níže navržená opatření vycházejí z jakéhosi rámce, představující soubor témat, které korespondují s tématickým rozsahem dotazníkového šetření. Opatření mají podobu spíše organizačního charakteru, protože technologická stránka informační bezpečnosti nebyla předmětem této práce. I z pohledu respondentů, kdy pro některé respondenty by bylo obtížné reagovat na příliš odborné dotazy. Dalším důvodem je, že organizační opatření, např. v podobě stanovení bezpečnostních politik, jsou mnohdy významnější než samotné investování do technologií. Bez stanovených organizačních pravidel jsou informační technologie lehce zranitelné.

[74] CIT VŠB-TU OSTRAVA. *Návrh ICT strategie VŠB-TUO*. Ostrava, 2013
[75] Tamtéž.

4.6.1 Větší informovanost o poskytování ICT služeb

Více poukazovat na možné problémy, přidat více informací o existujících směrnicích a pravidlech, týkajících se informační bezpečnosti. Studenti by měli být více informováni, např. prostřednictvím informačních e-mailů nebo aktualit na portálu univerzity, o nových dokumentech, zaměřených na informační bezpečnost. Z dotazníku vyplývá, že téměř 50% uživatelů by pravděpodobně ani nevědělo, na koho se obrátit v případě výskytu bezpečnostního incidentu v rámci univerzitní sítě a stejné množství respondentů se doposud neseznámilo se směrnicemi o bezpečnosti informací. Dalších 30% studentů dokonce ani neví, že nějaká pravidla a provozní řády existují.

4.6.2 Vytvoření e-learningového kurzu pro studenty a jeho opakování

Cílem je vytvoření e-learningového kurzu, který by se zaměřoval na problematiku informační bezpečnosti. Uživatelé by měli povinnost hned při prvním kontaktu s univerzitou (např. při zahájení školního roku) vyplnit tento kurz, jehož účelem by bylo zvýšit povědomí uživatelů o bezpečnostních opatřeních, hrozbách, včetně hrozeb plynoucích ze sociálního inženýrství, protože stále nejvíce útoků je způsobených selháním lidského faktorů. Tento kurz by byl zakončen testem, který ověří nabyté znalosti. Zároveň by kurz měl být v pravidelných intervalech opakován. Zvýšené povědomí o bezpečnostních aspektech by mohlo přispět k obezřetnějšímu chování uživatelů a lepšímu zabezpečení jejich zařízení, za účelem předejít bezpečnostním incidentům.

4.6.3 Rozšiřování bezdrátové sítě

Z dosažených výsledků analýzy lze konstatovat, že studenti považují bezdrátové připojení na univerzitě za důležité. Jedním z důvodů může být větší rozmach zařízení, které umožňují připojení do bezdrátové sítě a zároveň jejich dostupnost. I z pohledu cen těchto zařízení, jak notebooků, smartphonů i dnes oblíbených tabletů, se stále stávají pro uživatele cenově dostupnějšími. Proto by bylo vhodné postupně rozšiřovat bezdrátové sítě a pokrýt tak dosud nepokryté části univerzity, včetně volby vhodného autentizačního mechanismu. Stejně tak se věnovat postupné obnově zastaralých zařízení síťové infrastruktury.

4.6.4 Ukončování relací na kioscích

V rámci univerzity jsou na daných místech rozmístěny informační kiosky, představující bezdiskové počítače zabudované do speciálních kioskových skříní. Kioskový počítač poskytuje studentům a zaměstnancům základní ICT funkce a služby. Kiosek je dostupný pro všechny uživatele univerzity, jež se úspěšně identifikují prostřednictvím své identifikační karty. Na kiosek se mohou uživatelé přihlásit pomocí své identifikační karty. Řešením v oblasti informační bezpečnosti by bylo zavedení a snížení časového intervalu při neaktivitě přihlášeného uživatele. Po tomto časovém intervalu by došlo k automatickému odhlášení, a tím částečně eliminovat rizika spojené s neukončenou relací posledního přihlášeného uživatele.

4.6.5 Optimalizace prostředí pro využívané prohlížeče

V otázce používaných prohlížečů studenti nejvíce volili prohlížeče Google Chrome a Mozilla Firefox, přičemž první jmenovaný používá až 71% ze všech respondentů. Tímto se pouze potvrzuje rostoucí trend v oblíbenosti prohlížeče Google Chrome. V současnosti jsou všechna univerzitní portálová řešení optimalizována pouze pro prohlížeče Mozilla Firefox a Internet Explorer. Proto je velice důležité zaměřit se na optimalizaci webových aplikací také pro prohlížeč Google Chrome.

4.7 Bezpečnostní hrozby současnosti

Následující přehled obsahuje soupis největších současných bezpečnostních hrozeb, ve kterých odborníci vidí potenciální místa pro výskyt bezpečnostních incidentů.

4.7.1 Cílené a sofistikované mobilní útoky

Pokročilé přetrvávající hrozby (advanced persistent threats, APT) jsou definovány schopností využívat sofistikovanou technologii a více metod či vektorů šíření k tomu, aby dosáhly svého cíle a získaly citlivé, nebo rovnou tajné informace. Z poslední doby reprezentují tuto kategorii škodlivé kódy Stuxnet, Flame a Gauss. V roce 2013 lze předpokládat, že se podobné hrozby dostanou i do širší populace. Útočníci se poté, co získají hledané informace, snaží za sebou odstranit stopy i škodlivý kód tak, aby oběť neměla šanci zaregistrovat, že útok proběhnul.

Cílem útočníků budou kriminální aktivity, jako je vydírání nebo vyhrožování únikem informací v případě, že nebude zaplaceno odpovídající "výpalné".[76]

4.7.2 Dvoufaktorová autentizace

Bezpečnostní model založený jen na heslech je mrtvý. Dnes snadno dostupné nástroje dokážou rozbít heslo o délce čtyř nebo pěti znaků v řádu několika minut. Přihlašovací údaje uložené v zašifrovaných databázích (často napadané skrze webové portály a SQL injektáž) společně s bezdrátovou bezpečností (WPA2) budou populárním terčem útoků za využití cloudových služeb. Proto se předpokládá, že tento rok bude v organizacích ve znamení narůstající implementace dvoufaktorové autorizace pro zaměstnance i partnery. Bude se skládat z webového přihlašovacího rozhraní vyžadujícího uživatelské heslo společně se sekundárním heslem, které bude generováno na samostatném bezpečnostním tokenu nebo přijato na mobilní komunikační zařízení. Tato metoda patří k nejefektivnějšímu zabezpečení on-line aktivit.[77]

4.7.3 Exploity se zaměřením na komunikaci dvěma zařízeními (M2M)

Komunikace zařízení–zařízení (machine to machine, M2M) odkazuje na technologii, která umožňuje bezdrátově nebo s pomocí klasických sítí komunikaci mezi zařízeními. Zatímco praktické technologické možnosti M2M jsou úžasné a mají v mnoha případech potenciál odstranit lidskou chybu, přetrvává mnoho otazníků ohledně jejich bezpečnosti. Přepokládá se, že letos zaznamenáme první pokusy o napadení systémů M2M, velmi pravděpodobně na platformě spojené s národní bezpečností, jako je například objekt určený pro vývoj zbraní. Útok bude nejspíše provedený "otrávením" proudu informací, které putují komunikační linkou v rámci M2M. Jeden stroj pak zpracuje nekorektní informace, čímž dojde k otevření zranitelnosti a jejímu následnému zneužití útočníkem k přístupu ke zranitelnému bodu.[78]

[76] FORTINET. Předpověď bezpečnostních hrozeb pro rok 2013. *IT Systems: IT Security* [online]. 2013 [cit. 2013-04-21]. Dostupné z: http://www.systemonline.cz/it-security/predpoved-bezpecnostnich-hrozeb-pro-rok-2013.htm
[77] Tamtéž.
[78] Tamtéž.

4.7.4 Exploity dokážou obejít prostředí sandboxů

Sandboxy (virtuálně uzavřená a izolovaná prostředí) jsou využívány v bezpečnostních technologiích k oddělení programů a aplikací tak, aby případný škodlivý kód nemohl přejít z jednoho procesu (např. prohlížeče dokumentů) do druhého (např. operačního systému). K tomuto schématu už přistoupilo několik výrobců (jako třeba Adobe a Apple) a je velmi pravděpodobné, že se k nim brzy přidají další. S tím, jak se tato technologie stává rozšířenější, útočníci přirozeně začínají řešit i to, jak ji obejít. Šlo například o zranitelnost Adobe Reader X. Nejnověji objevené exploity se pokoušely zůstávat v "neviditelném" režimu a neměly žádné další projevy (což by nasvědčovalo tomu, že jsou zatím ve vývoji a že jde o testy), nebo se aktivně pokoušely hromadně obejít všechny technologie. Předpokládá se, že se v roce 2013 setkáme s inovativními kódy, které budou navržené k obejití izolovaných prostředí užívaných bezpečnostními aplikacemi a mobilními zařízeními.[79]

4.7.5 Meziplatformové botnety

Mobilní botnety, jako například Zitmo, mají většinu stejných vlastností a funkcionalit jako tradiční botnety pro PC. Lze proto očekávat, že v roce 2013 spatří díky tomuto sdílení vlastností mezi platformami nové formy útoků odepření služby DDoS (distributed denial of service), které souběžně využijí PC i mobilní zařízení. Pro představu: infikované mobilní zařízení a PC budou sdílet stejné ovládací a řídicí servery a protokol útoku a budou schopné zaútočit společně v jednom okamžiku. Díky tomu se možnosti botnetů znásobí. To, co byly dosud dvě oddělené sítě botnetů běžící jednak na PC, jednak na zařízeních s mobilními operačními systémy, jako je Android, se nyní stane jedním botnetem využívajícím různého druhu koncových bodů.[80]

4.7.6 Mobilní škodlivé kódy

Dnešní škodlivé kódy jsou vytvářené pro mobilní zařízení stejně jako pro stolní počítače a notebooky. Dosud přitom byla hlavním cílem pozornosti útočníků právě platforma klasických počítačů. A to proto, že jich bylo tolik, a že jsou na světě přece jen delší čas. Výzkumníci pozorují významný nárůst v objemu mobilních škodlivých kódů a předpokládají, že tento trend bude v letošním roce ještě dramatičtější. Mimo jiné zásluhou toho, že se dnes prodává

[79] FORTINET, ref. 76.
[80] Tamtéž.

více mobilních telefonů než notebooků nebo stolních PC. Lze očekávat, že bude ještě několik let trvat, než se počty škodlivých kódů pro mobilní zařízení srovnají s počty malware pro PC, objem malwaru pro mobilní platformy však bude do té doby dramaticky růst. Jeho tvůrci totiž dobře vědí, že zabezpečení mobilních zařízení je mnohem komplikovanější než zabezpečení tradičních počítačů.[81]

4.8 Desatero bezpečnosti informací

Existují různá doporučení a pravidla pro bezpečný pohyb uživatelů na Internetu a počítačové síti. Avšak následující přehled obsahuje deset základních bodů, které uživatelům radí, jak se chovat v případě bezpečnostních rizik a zároveň jak jim předcházet:[82]

- Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.
- Některé viry dokážou bezpečnostní software v PC zablokovat. Proto je vhodné pravidelně kontrolovat, zda funguje.
- Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.
- Pozor je nutné dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu.
- Při zadávání přístupových hesel na internetových stránkách je nutné kontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče, nebo tak, že adresa webové stránky začíná zkratkou **https**, kde „s“ znamená bezpečná.
- Citlivé osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.
- Do e-mailů nepatří důvěrné informace, jako je například číslo kreditní karty nebo heslo k bankovnímu účtu. Elektronickou poštu totiž může zachytit útočník.
- Firewall dovoluje lépe zabezpečit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.

[81] FORTINET, ref. 76.
[82] HOPSOFT. Antiviry [online]. 2012 [cit. 2013-04-17]. Dostupné z: http://www.hopsoft.cz/antiviry.php

- V internetových kavárnách a na cizích počítačích se nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalované keyloggery.
- Obezřetnost je nutná při připojení k nezašifrovaným bezdrátovým sítím. Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.

5 Závěr

Problémových oblastí v oboru informačních technologií existuje celá řada a odvíjí od využívaných prostředků a služeb. Proto je často komplikované a v podstatě nemožné věnovat se všem oblastem současně z důvodu omezených zdrojů, tedy jak finančních tak i lidských. Proto by mělo být v plné kompetenci hlavního správce univerzity, kterým je útvar CIT, vždy na dané období zvolit a realizovat vhodná opatření do stěžejních a problémových oblastí z pohledu informačních technologií univerzity. CIT v rámci svého působení každoročně sestavuje vlastní strategii, kde jsou zohledněny důležité aspekty a vize pro zajištění chodu univerzity v rámci IT, včetně bezpečnostních opatření.

Běžně se většina incidentů řeší až při jejich výskytu na půdě dané organizace. Proto je důležité zabývat se bezpečnostními opatřeními ještě dříve, než k nějakým incidentům dojde, a tím eliminovat škody, které mohou z těchto incidentů vyplynout. Podle novodobých trendů by měla být soustředěna pozornost především na mobilní zařízení a z nich plynoucí rizika.

Univerzitní prostředí je charakteristické velkým počtem lidi a je zapotřebí mít vždy na paměti potenciální problémy, které se mohou vyskytnout díky neopatrnému jednání uživatelů. Na druhou stranu máme uživatele, kteří se záměrně pokouší bezpečnostní opatření narušit a dostat se pomocí různých prostředků k citlivým informacím. Dle výsledků výroční zprávy univerzity dochází k meziročnímu nárůstu počtu zařízení, připojených do univerzitní bezdrátové sítě. Tento výsledek jen vypovídá o současném trendu v počtu využívaných zařízení uživateli. Bezdrátová síť tvoří zásadní část síťové infrastruktury univerzity a s jejím využíváním je spojena řada možných rizik. Proto je nutné v této oblasti sledovat aktuální trendy v zabezpečení, a pokud možno aplikovat takové bezpečnostní mechanismy, díky kterým lze eliminovat počet bezpečnostních incidentů. Průběžná inovace technické stránky sítě univerzity se pokládá za běžný proces v souladu s aktuálními technologiemi.

Diplomová práce se snaží poukázat na problematiku bezpečnosti informací, protože v současnosti neexistuje komplexní nástroj pro zabezpečení informací. Bezpečnost informací se většinou zajišťuje pomocí integrace několika dílčích řešení, které jako celek tvoří sadu nástrojů. Avšak tyto nástroje slouží jako prevence pro detekci či odstranění bezpečnostních hrozeb, a nezaručují dosažení dokonalé ochrany zařízení a infrastruktury. V této souvislosti je důležité zmínit podstatný problém, kdy zajištění bezpečnosti mnohdy závisí na samotném

chování uživatelů v rámci Internetu, informační společnosti a síťové infrastruktury. Lidský faktor stále patří mezi nejčastější příčiny bezpečnostních incidentů.

Dalším cílem bylo zdůraznit důležité aspekty týkající se informační bezpečnosti a zároveň poukázat na existující trendy a metody pro její zajištění, v podobě uznávaných praktik, metod, rámců, standardů a norem. Hlavní náplní práce byla analýza informační bezpečnosti v univerzitním prostředí z pohledu studentů VŠB-TU Ostrava. Získané výstupy jsou výsledkem dotazníkového šetření a dále byly zpracovány pomocí statistických softwarových nástrojů. Na základě získaných výsledků byl vytvořen přehled návrhů bezpečnostních opatření, který slouží jako rámec doporučení pro budoucí plány útvaru CIT. Po provedeném průzkumu a jeho následného rozboru, včetně návrhu opatření, lze konstatovat, že všechny cíle práce byly úspěšně naplněny.

Velice zajímavými výsledky jsou zjištění v oblasti důležitosti bezdrátových sítí na univerzitě, informovanosti a přístupu studentů ke směrnicím a pravidlům týkajících se bezpečnosti informací a jimi preferovaných internetových prohlížečů. Na základě dosažených výsledků z provedených analýz a použitých metod byly zjištěny většinou slabé až středně velké závislosti mezi sledovanými proměnnými. Proto by bylo vhodné pokračovat v dalším průzkumu s upravenou strukturou otázek, která vyplynula z výsledků prvního šetření. Poté by dotazník poskytoval detailnější data pro jejich rozbor a analýzu závislostí, které by jednoznačně potvrdily či vyvrátily zjištěné výstupy.

Mnohdy není důležité zabývat se technologickým rozvojem infrastruktury IT, ale trend se ubírá směrem k efektivnímu řízení IT jako nástroje podporujícího strategii organizace. Pozornost by tedy měla být věnována spíše organizačnímu zajištění IT v podobě definování bezpečnostních politik, pravidel, směrnic atd.

Seznam použité literatury

Monografické zdroje:

1. ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. V Tribunu EU vyd. 1. Brno: Tribun EU, 2009, 134 s. ISBN 978-80-7399-731-1.
2. ČSN ISO/IEC TR 13335-1. *Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT*. 1. vyd. Praha: Český normalizační institut, 1999. 24 s.
3. DOSTÁLEK, Libor a kol. *Velký průvodce protokoly TCP/IP: bezpečnost*. 2. aktualiz. vyd. Praha: Computer Press, 2003, 571 s. ISBN 80-722-6849-X.
4. DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
5. DRASTICH, Martin. *Systém managementu bezpečnosti informací*. 1. vyd. Praha: Grada, 2011, 126 s. Průvodce (Grada). ISBN 978-80-247-4251-9.
6. EGAN, Mark a Tim MATHER. *The executive guide to information security: threats, challenges, and solutions*. 1. vyd. Boston: Addison-Wesley Professional, 2004, 288 s. ISBN 978-03-213-0451-3.
7. GOGELA, Robert. *Pracovní příručka bezpečnostního manažera.* Vyd. 1. Praha: Česká pobočka AFCEA, 2011, 104 s. ISBN 978-80-7251-364-2.
8. KAFKA, Milan. *Význam ochrany a bezpečnosti IS-IT pro konkurenceschopnost podniku: The point of IS-IT protection and security for the firm competitiveness : teze disertační práce*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011, 36 s. ISBN 978-80-7454-036-3.
9. KALETA, Eduard. *Informační technologie: správa počítačových sítí*. 1. vyd. Praha: Professional Publishing, 2008, 180 s. Vzdělávání pro 21. století. ISBN 978-80-86946-61-0.
10. MAISNER, Martin. Odpovědnost za obsah přenosu v elektronických komunikacích. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2012, 133 s. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7357-964-7.

11. POŽÁR, Josef. *Manažerská informatika*. Plzeň: Aleš Čeněk, 2010, 357 s. ISBN 978-80-7380-276-9.
12. POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Vyd. 1. Praha: Vydavatelství PA ČR, 2007, 219 s. ISBN 978-80-7251-250-8.
13. SEDLÁČEK, Václav. *Management systému informační bezpečnosti - ISMS: studijní opora disciplíny*. Vyd. 1. Třebíč: Vivat Academia, 2010, 96 s. ISBN 978-80-87385-050.
14. STRNÁD, Ondrej. *Systém riadenia informačnej bezpečnosti: aplikovanie procesného riadenia : monografia*. 1. vyd. Ostrava: Amos, 2011, 241 s. Teória a prax riadenia informačnej bezpečnosti. ISBN 978-80-904766-6-0.
15. ŘÍHA, Milan a Ladislav SIEGER. *Bezpečnostní systémy*. Vyd. 4., aktualiz. Praha: Námořní akademie České republiky. ISBN 978-808-7103-326.

Elektronické zdroje:

16. CESNET. *CESNET* [online]. 2013 [cit. 2013-04-17]. Dostupné z: http://www.cesnet.cz/sdruzeni/
17. DROZD, Michal. Boj s lidským faktorem v informační bezpečnosti. *IT Systems* [online]. 2007 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/it-security/boj-s-lidskym-faktorem-v-informacni-bezpecnosti.htm
18. EDUROAM. *Eduroam.cz* [online]. 2012 [cit. 2013-04-17]. Dostupné z: http://www.eduroam.cz/
19. FORTINET. Předpověď bezpečnostních hrozeb pro rok 2013. *IT Systems: IT Security* [online]. 2013 [cit. 2013-04-21]. Dostupné z: http://www.systemonline.cz/it-security/predpoved-bezpecnostnich-hrozeb-pro-rok-2013.htm
20. GRYGÁREK, Petr. *Směrované a přepínané sítě* [online]. Ostrava [cit. 2013-04-17]. Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/bezpecnost-ucitele.pdf. FEI VŠB-TU Ostrava.
21. HANÁČEK, Jindřich. Vliv procesního řízení IT na snižování nákladů logistických firem. *IT Systems* [online]. 2010 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/it-pro-logistiku/vliv-procesniho-rizeni-it-na-snizovani-nakladu-logistickych-firem-1.htm

22. HLOBIL, Petr. Bezpečnost počítačových sítí (1): Úvod do problematiky. [online]. 2012 [cit. 2013-04-17]. Dostupné z: http://www.emersion.cz/25744n-bezpecnost-pocitacovych-siti-uvod-do-problematiky

23. HOLEK, Tomáš. Procesní řízení IT služeb. *IT Systems* [online]. 2007 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/sprava-it/procesni-rizeni-it-sluzeb.htm

24. HOPSOFT. Antiviry [online]. 2012 [cit. 2013-04-17]. Dostupné z: http://www.hopsoft.cz/antiviry.php

25. Internet Explorer blokuje podle NSS Labs sedmkrát více útoků než konkurence. *ICT Security* [online]. 2011 [cit. 2013-04-17]. Dostupné z: http://www.ictsecurity.cz/sk/security-bezpenos/internet-explorer-blokuje-podle-nss-labs-sedmkrat-vice-utok-ne-konkurence.html

26. ISACA. *An Introduction to the Business Model for Information Security* [online]. 2009 [cit. 2013-04-17]. Dostupné z: http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf

27. ISACA. *COBIT 5 for Information Security* [online]. 2012 [cit. 2013-04-17]. ISBN 978-1-60420-255-7. Dostupné z: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

28. ITIL - Bezpečnost IS/IT. [online]. [cit. 2013-04-17]. Dostupné z: http://itil.cz/index.php?id=1003

29. MATYSKA, Luděk. Bezdrátová síť Fakulty informatiky. *Zpravodaj ÚVT MU* [online]. 2002, XII, č. 3 [cit. 2013-04-17]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/clanky_tisk/236.pdf

30. Metodika COBIT: systematický přístup k řízení ICT. *IT Systems* [online]. 2005 [cit. 2013-04-17]. Dostupné z: http://www.systemonline.cz/clanky/metodika-cobit-systematicky-pristup-k-rizeni-ict.htm

31. Nástroje statistické analýzy. *Microsoft Corporation* [online]. [cit. 2013-04-17]. Dostupné z: http://office.microsoft.com/cs-cz/excel-help/nastroje-statisticke-analyzy-HP005203873.aspx

32. OPLUŠTILOVÁ, Irena a Michaela TULISOVÁ. Elementární statistické metody a jejich věcný význam: Regresní a korelační analýza. [online]. 2003 [cit. 2013-04-17]. Dostupné z: http://www.regionalka.wz.cz/reg%20info/Elementarni%20%20stat.%20metody.htm

33. RAC. *ISO/IEC 27001:2005* [online]. [cit. 2013-04-17]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27001

34. RAC. *ISO/IEC 27002:2005* [online]. [cit. 2013-04-17]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/27002

35. ROHLEDER, David. Bezdrátové sítě v prostředí MU. *Zpravodaj ÚVT MU* [online]. 2004, XIV, č. 3 [cit. 2013-04-17]. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/clanky_tisk/297.pdf

36. TUO_SME_09_001. *Řešení bezpečnostních IT incidentů na VŠB-TU Ostrava*. Ostrava: VŠB-TUO, 2009. Dostupné z: https://www.vsb.cz/share/uploadedfiles/secured/smernice/SME_09_001.pdf

37. VŠB-TU OSTRAVA. *Antivirová ochrana a IPS* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/sluzby/IPS/

38. VŠB-TU OSTRAVA. *Autorský zákon a počítačová síť VŠB-TU Ostrava* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/pravidla/az/

39. VŠB-TU OSTRAVA. *Eduroam - návštěvy na VŠB-TU Ostrava* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/sluzby/eduroam/visitors/

40. VŠB-TU OSTRAVA. *Výroční zpráva o činnosti VŠB - TUO za rok 2011* [online]. Ostrava, 2012 [cit. 2013-04-17]. Dostupné z: http://www.vsb.cz/miranda2/export/sites-root/intranet/innet/cs/okruhy/uredni-deska/vyrocni-zpravy-a-zamery/dokumenty/vz-cinnost-2011.pdf

41. VŠB-TU OSTRAVA. *WIFI - Bezdrátová síť VŠB-TU Ostrava* [online]. [cit. 2013-04-17]. Dostupné z: http://idoc.vsb.cz/cs/okruhy/cit/tuonet/sluzby/wifi/

42. *III. cvičení ze statistiky* [online]. Olomouc [cit. 2013-04-17]. Dostupné z: http://ulb.upol.cz/praktikum/statistika3.pdf. UPOL.

Ostatní zdroje:

43. CIT VŠB-TU OSTRAVA. *Návrh ICT strategie VŠB-TUO*. Ostrava, 2013. Interní dokument Centra informačních technologií VŠB-TU Ostrava.

Seznam zkratek

ACL	Access control list
AES	Advanced Encryption Standard
BMIS	Business Model for Information Security
BS	British Standard
CCTA	Central Computer and Telecommunications Agency
CESNET	Czech Education and Scientific Network
CIA	Confidentiality, Integrity and Availability
CIT	Centrum informačních technologií
CMM	Capability Maturity Model
COBIT	Control Objectives for Information and related Technology
CRAMM	CCTA Risk Analysis and Management Method
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
ČSN	české technické normy
DMZ	Demilitarizovaná zóna
DNS	Domain Name System
DoS	Denial of Service
DS	Deliver & Support
DSM	Data Security Management
eduroam	Education Roaming
FEI	Fakulta elektrotechniky a informatiky
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HW	hardware
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IS	informační systém

ISACA	Information Systems Audit and Control Association
ISG	Information Security Governance
ISMS	Information Security Management Systém
ISO	International Organization for Standardization
IT	informační technologie
ITIL	Information Technology Infrastructure Library
NBÚ	Národní bezpečnostní úřad
NIST	National Institute of Standards and Technology
NSS	Network Security Services
OBD	Osobní bibliografická databáze
OGC	Office Of Government Commerce
OS	operační systém
PDCA	Plan-Do-Check-Act
PMBOK	A Guide to the Project Management Body of Knowledge
PO	Plan & Organise
POP3	Post Office Protocol
PSIB	Průzkumu stavu informační bezpečnosti v ČR
SAP	Systems - Applications - Products in data processing
SMTP	Simple Mail Transfer Protocol
SPC	Superpočítačové centrum
SW	software
SYN	synchronise packet
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TR	Technical Report
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
URL	Unique Resource Locator
VPN	Virtual private network
VŠB-TUO	Vysoká škola báňská - Technická univerzita Ostrava
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WWW	World Wide Web

Seznam tabulek

Seznam grafů

Seznam obrázků

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 26. dubna 2013

.....

Bc. Martin Huf

Seznam příloh